H3C Fixed Port Campus Switches

Configuration Examples

This manual is applicable to the following switches and software versions:

H3C S6812[S6813] Switch Series (Release 6615P03 and later)

H3C S6550XE-HI Switch Series & S6525XE-HI Switch Series (Release 6008 and later)

H3C S6520X-HI[EI][SI] & S6520-SI & S5560X-HI & S5000-EI & MS4600 Switch Series (Release 6308 and later)

H3C S5850 Switch Series (Release 8005 and later)

H3C S5570S-EI Switch Series (Release 11xx)

H3C S5560X-EI Switch Series & H3C S5500V2-EI Switch Series (Release 6308 and later)

H3C S5500V3-SI Switch Series (except S5500V3-24P-SI and S5500V3-48P-SI switches) (Release 11xx)

ES5500 Switch Series (Release 6317P01 and later)

H3C S5170-EI Switch Series (Release 11xx)

H3C S5130S-EI[HI] Switch Series (Release 6308 and later)

H3C S5120V3-EI Switch Series and S5120V3-36F-SI & S5120V3-28P-HPWR-SI & S5120V3-54P-PWR-SI switches (Release 11xx)

H3C S5120V2-LI Switch Series and MS4300V2 & MS4320 & MS4320V2 Switch Series (Release 6308P01 and later)

WAS6000 Switch Series and WS5810-WiNet & WS5820-WiNet & WS5850-WiNet Switch Series (Release 6308P01 and later)

E500C & E500D Switch Series, S5560S-EI Switch Series, and S3100V3-EI[SI] Switch Series (Release 6309P01 and later)

H3C S5560S-SI Switch Series and MS4200 Switch Series (Release 6310 and later)

E128C & E152C switches and S5500V3-24P-SI & S5500V3-48P-SI switches (Release 6310 and later)

MS4520V2-30F Switch (Release 6312P01 and later)

MS4520V2-28S & MS4520V2-24TP switches (Release 6312P03 and later)

MS4520V2-30C & MS4520V2-54C switches (Release 6510P01 and later)

H3C S5110V2 & S5110V2-SI & S5130S-SI[LI] & S5120V2-SI & S5000V3-EI & S5000E-X Switch Series (Release 6310 and later)

H3C S5000V5-EI Switch Series (except S5008PV5-EI and S5008PV5-EI-HPWR switches) (Release 6319P01 and later)

IE4300-12P-AC & IE4300-12P-PWR switches, IE4300-M Switch Series, and IE4320 Switch Series (Release 6308P01 and later)

H3C S5000X-EI Switch Series, MS4320V3 Switch Series, S5120V3-LI Switch Series, and S5120V3-SI Switch Series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, S5120V3-54P-PWR-SI) (Release 6329 and later), H3C S3600V3-EI&S3600V3-SI Switch Series (Release 11xx), and H3C S5135S-EI Switch Series (Release 6658P01 and later)

Document version: 6W105-20240725

This manual is applicable to the following switches and software versions:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Contents

Introduction

This document provides login configuration examples. It also provides examples for implementing user access control by using command authorization and command accounting.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of login management.

Example: Configuring console login

Network configuration

Configure console login so users must pass local authentication to log in to the device through the console port.

Analysis

The port properties for the terminal emulation program must match the console port's default settings.

By default, a local user is assigned the user role **network-operator** and is not assigned any service type. To enable the user to log in through the console port, you must assign the **terminal** service type to the user. To enable the user to manage the device, you must assign the **network-admin** user role to the user.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release

	6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx

S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

For successful console port login, follow these restrictions and guidelines:

- Identify the console port carefully to make sure you are connecting to the correct port.
- Prepare a console terminal, for example, a PC. Make sure the console terminal has a terminal emulation program, such as HyperTerminal or PuTTY. For information about how to use terminal emulation programs, see the programs' user guides.

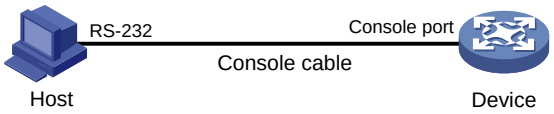
Procedures

1. Turn off the PC if the PC is on.
2. Connect the DB-9 female connector of the console cable to the serial port of the PC.
3. Identify the console port of the device carefully and connect the RJ-45 connector of the console cable to the console port.

IMPORTANT:

The serial ports on PCs do not support hot swapping. To connect a PC to an operating switch, first connect the PC end. To disconnect a PC from an operating device, first disconnect the device end.

Figure 1 Connecting a configuration terminal to the console port



4. Turn on the PC.
5. On the PC, launch the terminal emulation program, and create a connection that uses the serial port connected to the device. Set the port properties so the port properties match the following console port default settings:
   - **Bits per second**—9600 bps.
   - **Flow control**—None.
   - **Parity**—None.
   - **Stop bits**—1.
   - **Data bits**—8.
6. Power on the device and press **Enter** as prompted.

   The user view prompt appears. You can enter commands to configure or manage the device. To get help, enter **?**.
7. Configure AUX line 0:

   # Enter AUX line view.

   ```
   <Sysname> system-view
   [Sysname] line aux 0
   ```

   # Enable scheme authentication to use AAA to authenticate the console login user.

   ```
   [Sysname-line-aux0] authentication-mode scheme
   [Sysname-line-aux0] quit
   ```

   # Create the local user **admin**.

   ```
   [Sysname] local-user admin class manage
   New local user added.
   ```

   # Set the password to **hello12345** (plain text) for the local user.

   ```
   [Sysname-luser-manage-admin] password simple hello12345
   ```

   # Assign the **terminal** service type and the **network-admin** user role to the user. Reclaim the default user role.

   ```
   [Sysname-luser-manage-admin] service-type terminal
   [Sysname-luser-manage-admin] authorization-attribute user-role network-admin
   [Sysname-luser-manage-admin] undo authorization-attribute user-role
   network-operator
   [Sysname-luser-manage-admin] quit
   ```

Verifying the configuration

Log in to the device through the console port again, and press **Enter** and enter the username **admin** and password **hello12345** as prompted.

```
Line aux0 is available.


Press ENTER to get started.
Login: admin
Password:
```

```
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<Sysname>
```

Configuration files

```
#
line aux 0
 authentication-mode scheme
 user-role network-admin
#
local-user admin class manage
 password hash $h$6$RgG+mm4RKXICN1tY$ld6pV+qB2a/BBFXVnqocFJjYgx/EKCYod9tHmGRP8AA
1qnbeRcB6Bd4jW+cteG9aY2Gc+J8JqLHsWwvtnLyEAw==
 service-type terminal
 authorization-attribute user-role network-admin
#
```

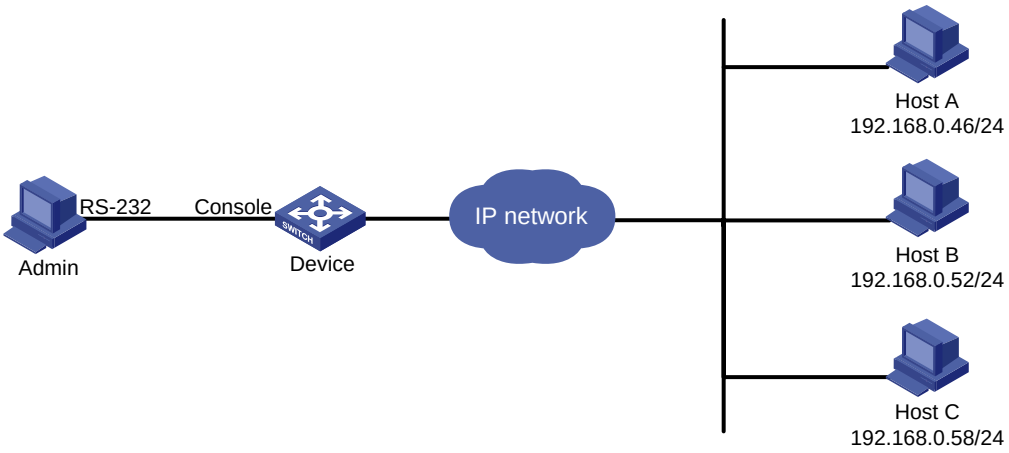
Example: Configuring user-role based Telnet login

Network configuration

As shown in Figure 2, users need to log in to the device remotely to manage the device.

- Configure Telnet login to enable users to Telnet to the device.
- Configure Telnet user authentication so a Telnet user must provide the correct username and password at login.
- Configure access control so only Telnet users at 192.168.0.46/24 and 192.168.0.52/24 can Telnet to the device.
- Configure two local users.
  - One local user can manage the device.
  - One local user can use only the read commands of features.

Figure 2 Network diagram



Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

To control Telnet login, configure an ACL to permit access only from the specified IP addresses.

By default, a local user is assigned the user role **network-operator**. To restrict a local user to read commands, you must create a user role that can access only read commands.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx

Hardware	Software version
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Log in to the device through the console port. (Details not shown.)

Enable Telnet service.

```
<Sysname> system-view
[Sysname] telnet server enable
```

Enable scheme authentication to use AAA to authenticate the Telnet login user.

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

Create the local user **userA**. Set the password to **hello12345** (plain text).

```
[Sysname] local-user userA class manage
New local user added.
[Sysname-luser-manage-userA] password simple hello12345
```

Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[Sysname-luser-manage-userA] authorization-attribute user-role network-admin
[Sysname-luser-manage-userA] service-type telnet
[Sysname-luser-manage-userA] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-userA] quit
```

Create user role **roleB**. Add rule 1 to permit the user role to access read commands of all features.

```
[Sysname] role name roleB
[Sysname-role-roleB] rule 1 permit read feature
[Sysname-role-roleB] quit
```

Create the local user **userB**. Set the password to **hello12345** (plain text).

```
[Sysname] local-user userB class manage
New local user added.
```

```
[Sysname-luser-manage-userB] password simple hello12345
```

Assign the Telnet service type and the **roleB** user role to the user. Reclaim the default user role.

```
[Sysname-luser-manage-userB] authorization-attribute user-role roleB
[Sysname-luser-manage-userB] service-type telnet
[Sysname-luser-manage-userB] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-userB] quit
```

Create ACL 2000 and add rules to permit only access from 192.168.0.46 and 192.168.0.52.

```
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 1 permit source 192.168.0.46 0
[Sysname-acl-ipv4-basic-2000] rule 2 permit source 192.168.0.52 0
[Sysname-acl-ipv4-basic-2000] rule 3 deny source any
[Sysname-acl-ipv4-basic-2000] quit
```

Apply the ACL to filter Telnet logins.

```
[Sysname] telnet server acl 2000
```

Verifying the configuration

1. Telnet to the device from Host A, and enter the username **userA** and password **hello12345** as prompted.
2. Display the commands available in user view.

   The commands for device configuration and management are included in the list.

```
Login: userA
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname> ?
User view commands:
  archive             Archive configuration
  arp                 Address Resolution Protocol (ARP) module
  backup              Backup operation
  boot-loader         Software image file management
  bootrom             Update/read/backup/restore bootrom
  cd                  Change current directory
  cfd                 Connectivity Fault Detection (CFD) module
  clock               Specify the system clock
  copy                Copy a file
  create              Create a file
  debugging           Enable system debugging functions
  delete              Delete a file
  diagnostic-logfile  Diagnostic log file configuration
  dir                 Display files and directories on the storage media
  display             Display current system information
  erase               Alias for 'delete'
```

```
  exception           Exception information configuration
  exit                Alias for 'quit'
  fdisk               Partition a storage medium
  fixdisk             Check and repair a storage medium
  format              Format a storage medium
  free                Release a connection
  ftp                 Open an FTP connection
---- More ----
```

3. Telnet to the device from Host B, and enter the username **userB** and password **hello12345** as prompted.
4. Display the commands available in user view.

   Only read commands are displayed.

```
Login: userB
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname> ?
User view commands:
  dir          Display files and directories on the storage media
  display      Display current system information
  erase        Alias for 'delete'
  exit         Alias for 'quit'
  md5sum       Compute the hash digest of a file using the MD5 algorithm
  more         Display the contents of a file
  no           Alias for 'undo'
  pwd          Display current working directory
  quit         Exit from current command view
  sha256sum    Compute the hash digest of a file using the SHA256 algorithm
  show         Alias for 'display'
  system-view  Enter the System View
  write        Alias for 'save'

<Sysname>
```

5. Telnet to the device from Host C.

   Your access request is rejected.

Configuration files

```
#
 telnet server enable
 telnet server acl 2000
#
acl basic 2000
 rule 1 permit source 192.168.0.46 0
```

```
 rule 2 permit source 192.168.0.52 0
 rule 3 deny
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
local-user userA class manage
 password hash $h$6$I2Sg4Llj1qVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
 service-type telnet
 authorization-attribute user-role network-admin
#
local-user userB class manage
 password hash $h$6$q+c3OcSxrPpDpsDf$BWkgfOyxBLyR5zyYgF/+VvN/1ofy81zoHDlFf80OjDl
a6/EiSJbSBl33PeazilSkWSYcttkg5v5bGecB7oYwAw==
 service-type telnet
 authorization-attribute user-role roleB
#
role name roleB
 rule 1 permit read feature
#
```

Example: Configuring login user command authorization and accounting

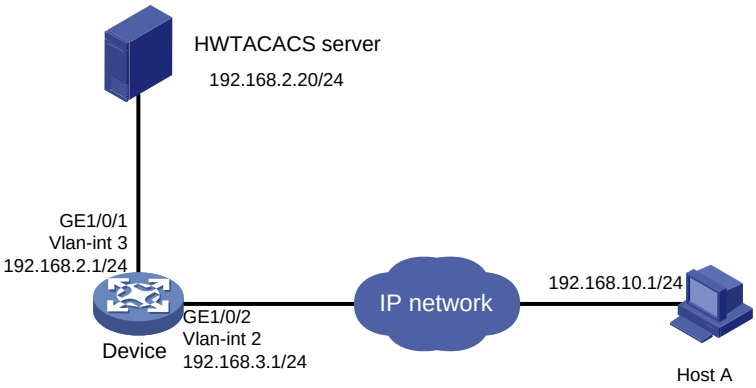
Network configuration

As shown in Figure 3, Host A needs to log in to the device to manage the device.

For device security purposes, configure the device to perform the following tasks:

- Allow Host A to Telnet in after authentication.
- Use the HWTACACS server to control the commands that the user can execute.
- Send commands executed by users to the HWTACACS server to monitor and control user operations on the device.

Figure 3 Network diagram



Analysis

To implement command authorization and accounting, you must perform the following tasks:

- Enable scheme authentication and configure a HWTACACS scheme on the device.
- Configure an account on the HWTACACS server for the Telnet user and assign commands for the user to use.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release

S6520X-EI switch series	6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx

MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

The command authorization function takes effect immediately after you execute the **`command authorization`** command. Before executing this command, you must complete the following tasks:

- Configure a user account on the HWTACACS server and specify the commands for the user to use.
- Configure the required HWTACACS scheme on the device.

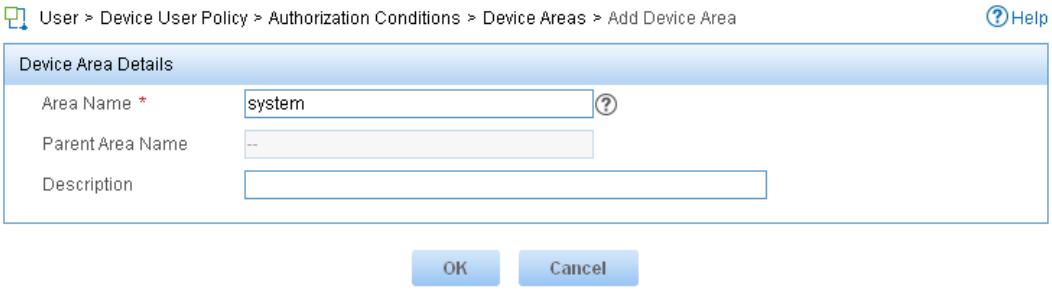
Procedures

Configuring the HWTACACS server

In this example, the HWTACACS server runs on IMC PLAT 7.1 (E0302) and IMC EIA 7.1 (E0301).

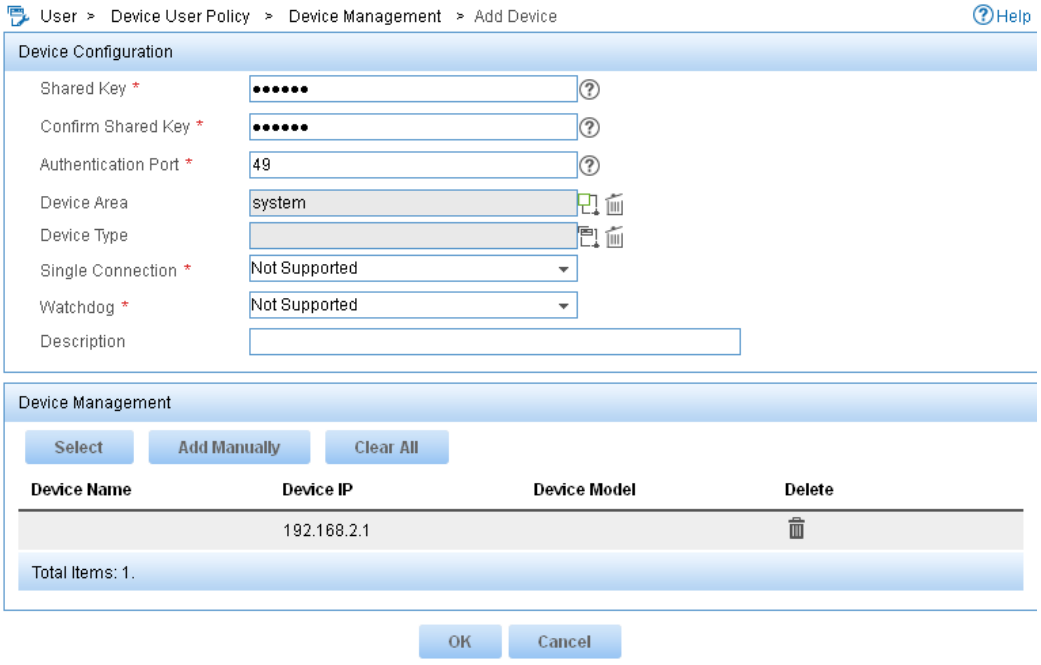
1. Add a device area:
   a. Log in to IMC.
   b. Click the **User** tab.
   c. From the navigation tree, select **Device User Policy** > **Authorization Conditions** > **Device Areas**.
   d. Click **Add**.
   e. Set the area name to **system** and click **OK**.

Figure 4 Adding a device area



2. Add a device:
   a. From the navigation tree, select **Device User Policy** > **Device Management**.
   b. Click **Add**.
   c. Enter **expert** for both **Shared Key** and **Confirm Shared Key**.
   d. Set the authentication port to **49**.
   e. Select the device area **system**.
   f. Select **Not Supported** for **Single Connection** to disable establishing multiple sessions over a single TCP connection.
   g. Select **Not Supported** for **Watchdog** to disable the device from sending watchdog packets while the user is online.
   h. In the **Device Management** area, click **Add Manually**.
   i. Enter the IP address **192.168.2.1** and click **OK**.
   j. Click **OK**.

Figure 5 Adding a device



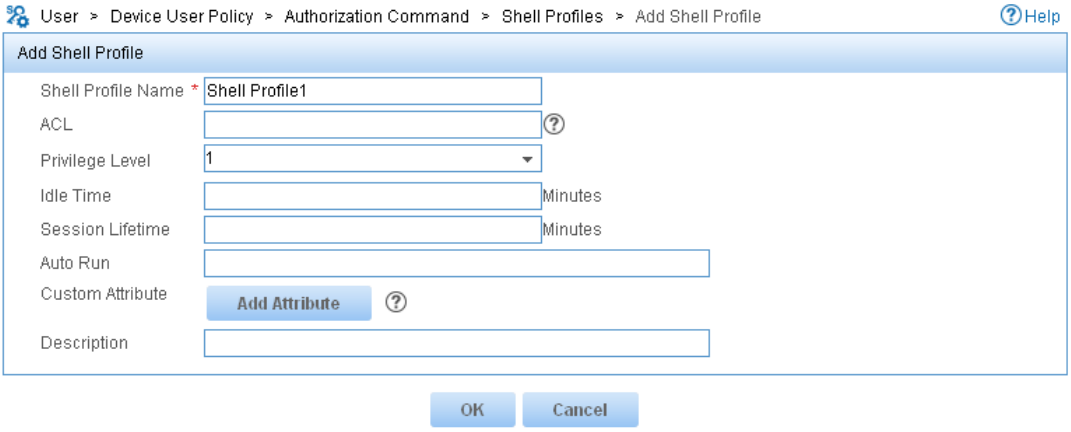
3. Add a shell profile:
   a. From the navigation tree, select **Device User Policy** > **Authorization Command** > **Shell Profiles**.
   b. Click **Add**.

c. Enter the profile name **Shell Profile1**.

d. Select the privilege Level **1**.

e. Click **OK**.

Figure 6 Adding a shell profile



4. Add an authorization policy:

a. From the navigation tree, select **Device User Policy** > **Authorization Policies**.

b. Click **Add**.

c. Enter the policy name **tac**.

d. In the **Access Authorization Info** area, click **Add** to configure access authorization information.

e. Select **system** for **Device Area**, **Unlimited** for **Device Type** and **Authorized Time Range**.

f. Select the shell profile **Shell Profile1**.

g. Select **Unlimited** for **Authorization Command Set** and click **OK**.

h. Click **OK**.

Figure 7 Configuring access authorization information

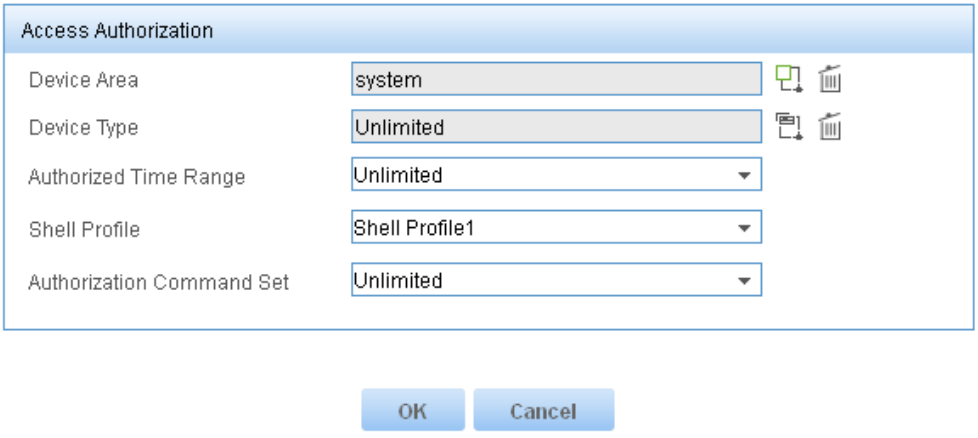
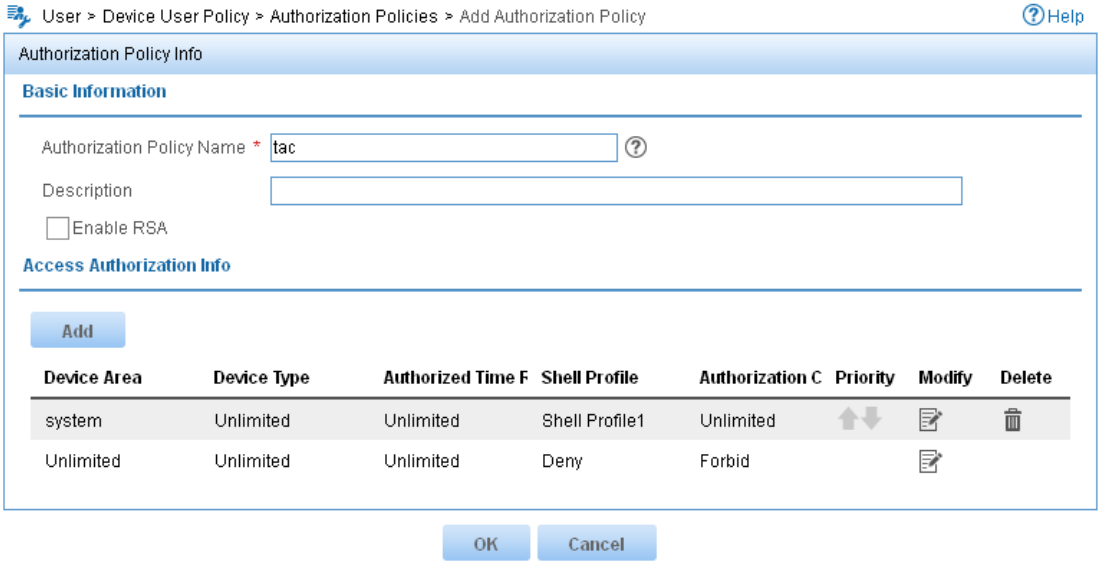
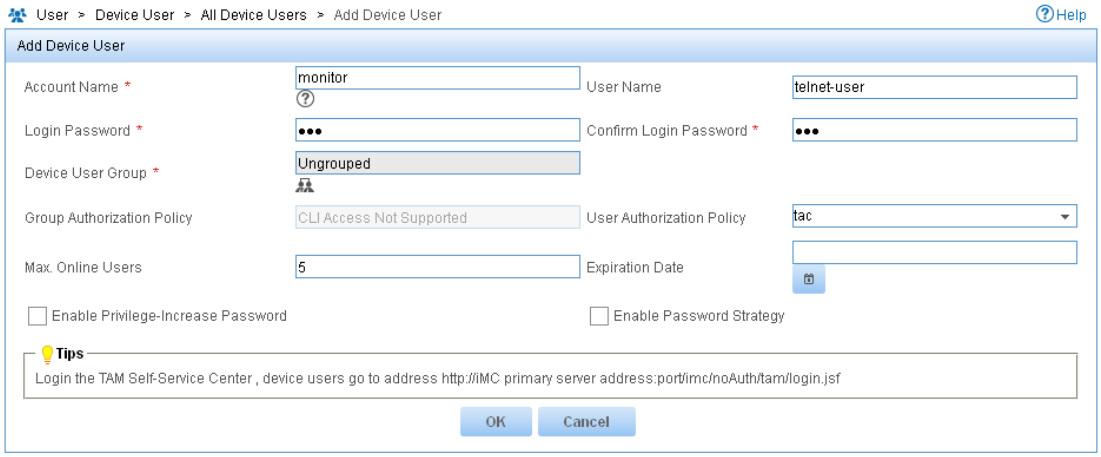


Figure 8 Adding an authorization policy



5. Add a device user:
   a. From the navigation tree, select **Device User** > **All Device Users**.
   b. Click **Add**.
   c. Enter the account name **monitor** and username **telnet-user**.
   d. Enter the login password **hello12345** and confirm the password.
   e. Select the user authorization policy **tac**.
   f. Enter **5** for **Max. Online Users** to limit the number of online users that use the account.
   g. Click **OK**.

Figure 9 Adding a device user



Configuring the device

Assign IP addresses to relevant interfaces. Make sure the device and the HWTACACS server can reach each other, and the device and Host A can reach each other. (Details not shown.)

Enable Telnet service.

```
<Sysname> system-view
```

```
[Sysname] telnet server enable
```

Create the HWTACACS scheme **tac**.

```
[Sysname] hwtacacs scheme tac
Create a new HWTACACS scheme.
```

Configure the scheme to use the HWTACACS server at 192.168.2.20:49 for authentication, authorization, and accounting.

```
[Sysname-hwtacacs-tac] primary authentication 192.168.2.20 49
[Sysname-hwtacacs-tac] primary authorization 192.168.2.20 49
[Sysname-hwtacacs-tac] primary accounting 192.168.2.20 49
```

Set the shared keys to **expert**.

```
[Sysname-hwtacacs-tac] key authentication simple expert
[Sysname-hwtacacs-tac] key authorization simple expert
[Sysname-hwtacacs-tac] key accounting simple expert
```

Remove domain names from usernames sent to the HWTACACS server.

```
[Sysname-hwtacacs-tac] user-name-format without-domain
[Sysname-hwtacacs-tac] quit
```

Configure the system-predefined domain **system**.

```
[Sysname] domain system
```

Use the HWTACACS scheme **tac** for login user authentication, authorization, and accounting. Use local authentication, authorization, and accounting as the backup method.

```
[Sysname-isp-system] authentication login hwtacacs-scheme tac local
[Sysname-isp-system] authorization login hwtacacs-scheme tac local
[Sysname-isp-system] accounting login hwtacacs-scheme tac local
```

Use the HWTACACS scheme **tac** for command authorization and accounting. Use local authorization as the backup command authorization method.

```
[Sysname-isp-system] authorization command hwtacacs-scheme tac local
[Sysname-isp-system] accounting command hwtacacs-scheme tac
[Sysname-isp-system] quit
```

Create the local user **monitor**. Set the password to **hello12345** (plain text).

```
[Sysname] local-user monitor class manage
New local user added.
[Sysname-luser-manage-monitor] password simple hello12345
```

Assign the Telnet service type and the **level-1** user role to the user. Reclaim the default user role.

```
[Sysname-luser-manage-monitor] service-type telnet
[Sysname-luser-manage-monitor] authorization-attribute user-role level-1
[Sysname-luser-manage-monitor] undo authorization-attribute user-role network-operator
[Sysname-luser-manage-monitor] quit
```

Enable scheme authentication to use AAA to authenticate the Telnet login user.

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
```

Enable command authorization and command accounting.

```
[Sysname-line-vty0-63] command authorization
[Sysname-line-vty0-63] command accounting
[Sysname-line-vty0-63] quit
```

Verifying the configuration

1. Verify the command authorization feature:

   # Telnet to the device, and enter the username **monitor** and password **hello12345**.

```
C:\Documents and Settings\Administrator> telnet 192.168.2.1

Login: monitor
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

   # Display commands available in user view and system view. Only commands permitted by the level-1 user role are displayed.

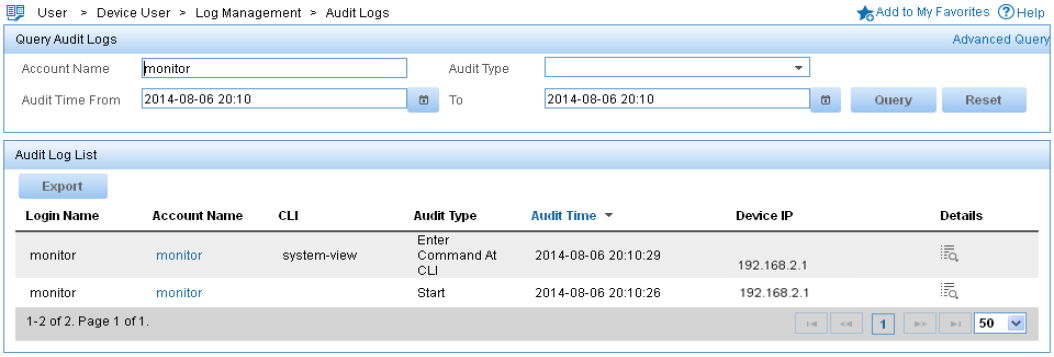
```
<Sysname> ?
User view commands:
  display      Display current system information
  erase        Alias for 'delete'
  exit         Alias for 'quit'
  mtrace       Configure the multicast traceroute
  no           Alias for 'undo'
  ping         Ping function
  quit         Exit from current command view
  show         Alias for 'display'
  ssh2         Establish an Stelnet connection to an Stelnet server
  super        Switch to a user role
  system-view  Enter the System View
  telnet       Establish a telnet connection
  tracert      Tracert function
  write        Alias for 'save'

<Sysname> system-view
[Sysname] ?
System view commands:
  access-list  Alias for 'acl'
  display      Display current system information
  end          Alias for 'return'
  erase        Alias for 'delete'
  exit         Alias for 'quit'
  hostname     Alias for 'sysname'
  logging      Alias for 'info-center'
  mtrace       Configure the multicast traceroute
  no           Alias for 'undo'
  ping         Ping function
  quit         Exit from current command view
  return       Exit to User View
  show         Alias for 'display'
```

```
tracert      Tracert function
write        Alias for 'save'
```

2. Verify the command accounting feature:
   a. Log in to IMC.
   b. Click the **User** tab.
   c. From the navigation tree, select **Device User** > **Log Management** > **Audit Logs**.
   d. In the **Query Audit Logs** area, enter the account name **monitor**, select the audit time range, and click **Query**.

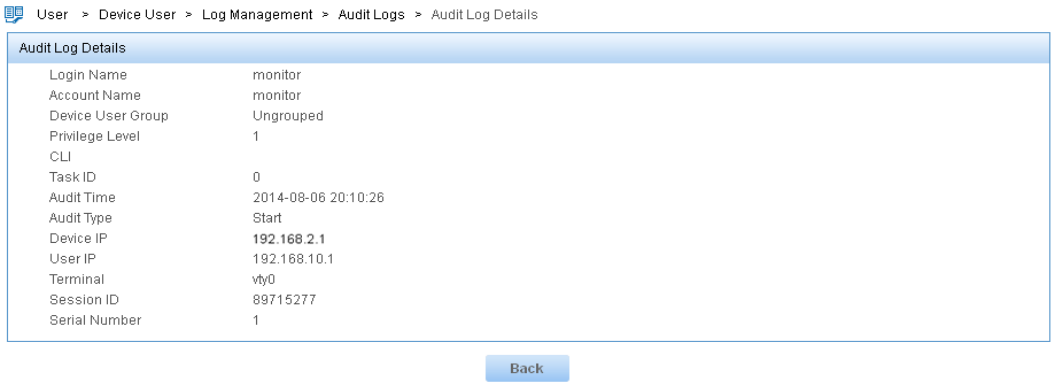
      A log for user **monitor** shows that the user executed the **`system-view`** command.

      Figure 10 Querying audit logs



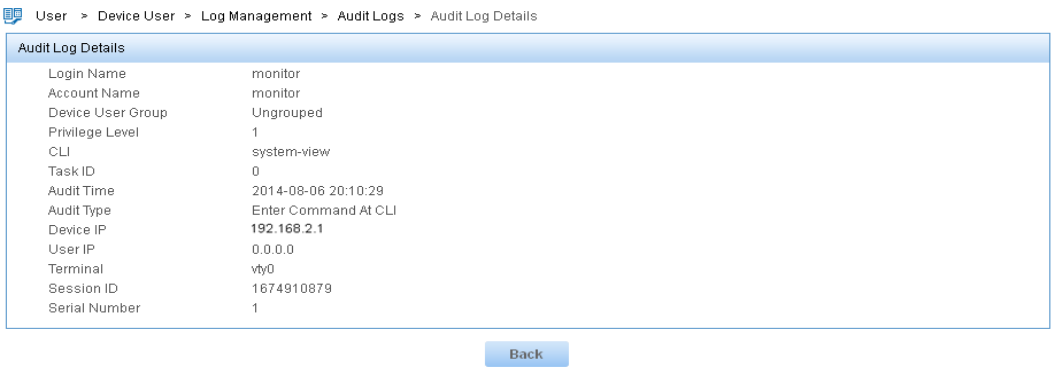
   e. Click the **Details** icon for the log of the **Start** audit type.

      Figure 11 Displaying details about the log of the Start audit type



   f. Click the **Details** icon for the log of the **Enter Command At CLI** audit type.

      Figure 12 Displaying details about the log of the Enter Command At CLI audit type



Configuration files

```
#
 telnet server enable
#
hwtacacs scheme tac
 primary authentication 192.168.2.20
 primary authorization 192.168.2.20
 primary accounting 192.168.2.20
 key authentication cipher $c$3$Fl1Mn3wBsh+vH6otPvoz+AdE7VaNS3c0Pw==
 key authorization cipher $c$3$2x6XI5xU7UGX6VqWFXNp2n3FG07uTNjiQw==
 key accounting cipher $c$3$2oKsuCOAZX1+3ibvTPxnJ1YvJ1MHqv73Lw==
 user-name-format without-domain
#
domain system
 authentication login hwtacacs-scheme tac local
 authorization login hwtacacs-scheme tac local
 accounting login hwtacacs-scheme tac local
 authorization command hwtacacs-scheme tac local
 accounting command hwtacacs-scheme tac
#
local-user monitor class manage
 password hash $h$6$5BqWnAJTpBbU5NbY$PbdgF+43eE5WMvj2iHPySfd5nGqj5AhDCDOXTiUMJvR
FFVsZaF8EW1tgpsQPRSq7SDKaGqwHTy9nsabAoGNaYg==
 service-type telnet
 authorization-attribute user-role level-1
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
 idle-timeout 0 0
 command authorization
 command accounting
#
```

Example: Configuring Telnet login

Network configuration

As shown in Figure 13, users need to log in to the device remotely to manage the device.

- Configure Telnet login to enable users to Telnet to the device.
- Configure Telnet user authentication so a Telnet user must provide the correct username and password at login.
- Configure the device to send up to 20 lines to the configuration terminal at a time.
- Set the command history buffer size to 100.

- Set the maximum number of concurrent Telnet users to 10.
- Set the session idle timeout to 20 minutes.

Figure 13 Network diagram

Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

By default, a local user is assigned the user role **network-operator**. To allow the user to use all commands on the device, assign the user role **network-admin** to the user.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx

WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Log in to the device through the console port. (Details not shown.)

Change the device name and enable Telnet service.

```
<Sysname> system-view
[Sysname] sysname Device
[Device] telnet server enable
```

Assign IP addresses to interfaces.

```
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/1
[Device-vlan2] quit
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.3.1 24
[Device-Vlan-interface2] quit
```

Enable scheme authentication to use AAA to authenticate the Telnet login user.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Configure common VTY line settings.

```
[Device-line-vty0-63] screen-length 20
[Device-line-vty0-63] history-command max-size 100
[Device-line-vty0-63] idle-timeout 20
[Device-line-vty0-63] quit
```

Set the maximum number of concurrent Telnet users to 10.

```
[Device] aaa session-limit telnet 10
```

Create the local user **test**. Set the password to **hello12345** (plain text).

```
[Device] local-user test class manage
New local user added.
[Device-luser-manage-test] password simple hello12345
```

Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[Device-luser-manage-test] service-type telnet
[Device-luser-manage-test] authorization-attribute user-role network-admin
[Device-luser-manage-test] undo authorization-attribute user-role network-operator
```

```
[Device-luser-manage-test] quit
```

Verifying the configuration

1. Telnet to the device from Host A, and enter the username **test** and password **hello12345**.

   If the number of online Telnet users is less than 20, you are logged in to the system.

   ```
   Login: test
   Password:
   ******************************************************************************
   * Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
   * Without the owner's prior written consent,                                  *
   * no decompiling or reverse-engineering shall be allowed.                     *
   ******************************************************************************


   <Device>
   ```

   If the number of concurrent Telnet users has reached the maximum number, an error message is displayed.

   ```
   C:\Users\zhangsan>telnet 192.168.3.1
   Trying 192.168.3.1 ...
   Press CTRL+K to abort
   Connected to 192.168.3.1 ...

   The connection was closed by the remote host!
   ```

2. After login, do not perform any operations within 20 minutes.

   You are logged out.

   ```
   Inactive timeout reached, logging out.

   The connection was closed by the remote host!
   ```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 sysname Device
#
telnet server enable
#
interface Vlan-interface2
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
```

```
 authentication-mode scheme
user-role network-operator
 idle-timeout 20 0
 screen-length 20
 history-command max-size 100
#
aaa session-limit telnet 10
#
local-user test class manage
 password hash $h$6$/Xa6qIOrThQEVqbK$C00MPM5UaYoigaOfflWhpTskb/uB80yZ9O06tpztnDe
vrFEHqkvxfkSb4hUadHuknPSnjLNQByztfr30cP/Hlg==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

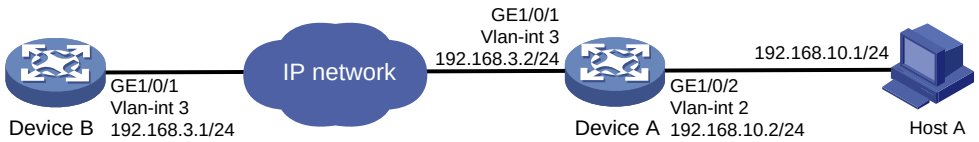
Example: Telnetting from the device to another device

Network configuration

As shown in Figure 14, the user connected to Device A needs to Telnet to Device B to manage Device B.

- Configure Telnet login to enable users to Telnet to Device A and Device B.
- Configure Telnet user authentication on Device A so a Telnet user must provide the correct username and password to log in to Device A.
- Configure access control so only Telnet users at 192.168.10.1/24 can Telnet to Device A and only Device A can Telnet to Device B.
- Configure the devices to send up to 20 lines to the configuration terminal at a time.
- Set the command history buffer size to 100.
- Set the session idle timeout to 20 minutes.

Figure 14 Network diagram



Analysis

Telnet service is disabled by default. To enable Telnet login, you must enable Telnet service.

By default, a local user is assigned the default user role **network-operator**. To allow the user to use all commands on the device, assign the user role **network-admin** to the user.

To control Telnet login, configure an ACL on each device to permit access only from the specified IP address.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Device A

Log in to Device A through the console port. (Details not shown.)

Change the device name and enable Telnet service.

```
<Sysname> system-view
[Sysname] sysname DeviceA
[DeviceA] telnet server enable
```

Assign IP addresses to interfaces.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/1
[DeviceA-vlan3] quit
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 192.168.3.2 24
[DeviceA-Vlan-interface3] quit
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.10.2 24
[DeviceA-Vlan-interface2] quit
```

Enable scheme authentication to use AAA to authenticate the Telnet login user.

```
[DeviceA] line vty 0 63
[DeviceA-line-vty0-63] authentication-mode scheme
```

Configure common VTY line settings.

```
[DeviceA-line-vty0-63] screen-length 20
[DeviceA-line-vty0-63] history-command max-size 100
[DeviceA-line-vty0-63] idle-timeout 20
[DeviceA-line-vty0-63] protocol inbound telnet
[DeviceA-line-vty0-63] quit
```

Create the local user **test**. Set the password to **hello12345** (plain text).

```
[DeviceA] local-user test class manage
New local user added.
[DeviceA-luser-manage-test] password simple hello12345
```

Assign the Telnet service type and the **network-admin** user role to the user. Reclaim the default user role.

```
[DeviceA-luser-manage-test] service-type telnet
[DeviceA-luser-manage-test] authorization-attribute user-role network-admin
[DeviceA-luser-manage-test] undo authorization-attribute user-role network-operator
[DeviceA-luser-manage-test] quit
```

Create ACL 2000 and add rules to permit only access from 192.168.10.1.

```
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule 1 permit source 192.168.10.1 0
[DeviceA-acl-ipv4-basic-2000] rule 2 deny source any
[DeviceA-acl-ipv4-basic-2000] quit
```

Apply the ACL to filter Telnet logins.

```
[DeviceA] telnet server acl 2000
```

Configuring Device B

Log in to Device B through the console port. (Details not shown.)

Change the device name and enable Telnet service.

```
<Sysname> system-view
[Sysname] sysname DeviceB
[DeviceB] telnet server enable
```

Assign IP addresses to interfaces.

```
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/1
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 192.168.3.1 24
[DeviceB-Vlan-interface3] quit
```

Disable authentication for the Telnet login user.

```
[DeviceB] line vty 0 63
[DeviceB-line-vty0-63] authentication-mode none
```

Configure common VTY line settings.

```
[DeviceB-line-vty0-63] screen-length 20
[DeviceB-line-vty0-63] history-command max-size 100
[DeviceB-line-vty0-63] idle-timeout 20
[DeviceB-line-vty0-63] protocol inbound telnet
[DeviceB-line-vty0-63] quit
```

Create ACL 2000 and add rules to permit only access from 192.168.3.2.

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule 1 permit source 192.168.3.2 0
[DeviceB-acl-ipv4-basic-2000] rule 2 deny source any
[DeviceB-acl-ipv4-basic-2000] quit
```

Apply the ACL to filter Telnet logins.

```
[DeviceB] telnet server acl 2000
```

Verifying the configuration

1. Telnet to Device A from Host A and enter the username **test** and password **hello12345**. You are logged in to the system.

```
Login: test
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<DeviceA>
```

If you use another host to Telnet to Device A, your access request is rejected.

```
C:\Users\zhangsan>telnet 192.168.10.2
Trying 192.168.10.2 ...
Press CTRL+K to abort
Connected to 192.168.10.2 ...
Failed to connect to the remote host!
```

2. After login, do not perform any operations in 20 minutes.

   You are logged out.

```
<DeviceA>
Inactive timeout reached, logging out.

The connection was closed by the remote host!
```

3. Telnet from Device A to Device B.

   You are logged in to the system.

```
<DeviceA>telnet 192.168.3.1
Trying 192.168.3.1 ...
Press CTRL+K to abort
Connected to 192.168.3.1 ...
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<DeviceB>
```

   If you use another host or device to Telnet to Device B, your access request is rejected.

```
<Device> telnet 192.168.3.1
Trying 192.168.3.1 ...
Press CTRL+K to abort
Connected to 192.168.3.1 ...
Failed to connect to the remote host!
```

4. After login, do not perform any operations within 20 minutes.

   You are logged out.

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
 telnet server enable
 telnet server acl 2000
#
interface Vlan-interface2
```

```
 ip address 192.168.10.2 255.255.255.0
#
interface Vlan-interface3
 ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
 protocol inbound telnet
 idle-timeout 20 0
 screen-length 20
 history-command max-size 100
#
acl basic 2000
 rule 1 permit source 192.168.10.1 0
 rule 2 deny source any
#
local-user test class manage
 password hash $h$6$V5dw8qzFDLAOmDzx$upf9K29n110G6OGdSXI0t69IoE5eot/Qh9Iuv/hptq6
2vxUq3867QbUBzmc6/hHwIfVQcDC8gVWpGvDQWXQTSQ==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

- Device B:

```
#
 sysname DeviceB
#
 telnet server enable
 telnet server acl 2000
#
interface Vlan-interface3
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode none
 user-role network-operator
```

```
 protocol inbound telnet
 idle-timeout 20 0
 screen-length 20
 history-command max-size 100
#
acl basic 2000
 rule 1 permit source 192.168.3.2 0
 rule 2 deny source any
#
```

Contents

Introduction

This document provides role-based access control (RBAC) examples to control access permissions of login users.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of RBAC.

Example: Configuring Telnet user to have access to read and write commands of specific features

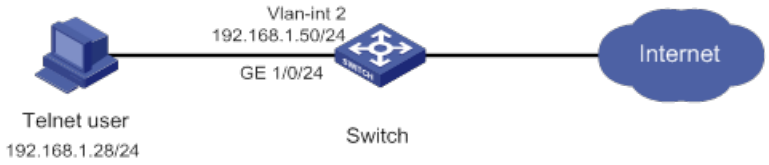
Network configuration

As shown in Figure 1, configure the switch to meet the following requirements:

- The Telnet user is authenticated on the switch in ISP domain **bbb**.
- The Telnet user is allowed to execute the read and write commands of the **ospf** and **filesystem** features after the user passes authentication.

Add a user account named **telnetuser** on the switch for the Telnet user, and set the user password to **hello12345**.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create a user role and configure rules for it. This allows the user role to have access permission to the required commands.
- Assign the user role to the Telnet user, so the Telnet user can obtain the required access permissions.
- Remove the default user role from the Telnet user, so the user can only have the access permissions of the configured user role.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure RBAC for local AAA users, follow these restrictions and guidelines:

- An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- You can create multiple rules for a user role. Each rule is uniquely identified by the rule number. A user role can access all commands permitted by the user role rules.
- If two user-defined rules conflict, the rule with the higher number takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**

Procedures

1. Configure VLAN settings:

   # Create VLAN 2.

   ```
   <Switch> system-view
   [Switch] vlan 2
   [Switch-vlan2] quit
   ```

   # Assign GigabitEthernet 1/0/24 (the interface connected to the Telnet user) to VLAN 2.

   ```
   [Switch] interface gigabitethernet 1/0/24
   [Switch-GigabitEthernet1/0/24] port access vlan 2
   [Switch-GigabitEthernet1/0/24] quit
   ```

   # Assign an IP address to VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] ip address 192.168.1.50 24
   [Switch-Vlan-interface2] quit
   ```

2. Configure the user login authentication method:

   # Enable Telnet server.

   ```
   [Switch] telnet server enable
   ```

   # Enable scheme authentication on user lines VTY 0 through VTY 63.

   ```
   [Switch] line vty 0 63
   [Switch-line-vty0-63] authentication-mode scheme
   [Switch-line-vty0-63] quit
   ```

3. Configure the authentication domain:

   # Create ISP domain **bbb** and enter ISP domain view.

   ```
   [Switch] domain bbb
   ```

   # Configure the authentication and authorization methods as **local** for login users in the domain.

   ```
   [Switch-isp-bbb] authentication login local
   [Switch-isp-bbb] authorization login local
   [Switch-isp-bbb] quit
   ```

4. Configure device management user **telnetuser**:

Create device management user **telnetuser** and enter local user view.

```
[Switch] local-user telnetuser class manage
```

Set the user password to **hello12345** in plain text.

```
[Switch-luser-manage-telnetuser] password simple hello12345
```

Specify the service type as Telnet.

```
[Switch-luser-manage-telnetuser] service-type telnet
[Switch-luser-manage-telnetuser] quit
```

5. Configure user role **role1**:

Create user role **role1** and enter user role view.

```
[Switch] role name role1
```

Configure rule 1 to permit the user role to access the read and write commands of the **ospf** feature.

```
[Switch-role-role1] rule 1 permit read write feature ospf
```

Configure rule 2 to permit the user role to access the read and write commands of the **filesystem** feature.

```
[Switch-role-role1] rule 2 permit read write feature filesystem
[Switch-role-role1] quit
```

6. Assign user role **role1** to device management user **telnetuser**:

Enter the view of the device management user.

```
[Switch] local-user telnetuser class manage
```

Assign user role **role1** to the user.

```
[Switch-luser-manage-telnetuser] authorization-attribute user-role role1
```

Remove the default user role **network-operator** from the user.

```
[Switch-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser] quit
```

Verifying the configuration

1. Display information about the user role **role1**.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RW-   feature       ospf
  2       permit RW-   feature       filesystem
  R:Read W:Write X:Execute
```

2. Verify that you can Telnet to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
```

```
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                  *
* no decompiling or reverse-engineering shall be allowed.                     *
******************************************************************************

<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

Verify that you can execute the write commands of the **ospf** feature. For example, configure OSPF.

```
<Switch> system-view
[Switch] ospf 1
[Switch-ospf-1] area 0
[Switch-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[Switch-ospf-1-area-0.0.0.0] quit
[Switch-ospf-1] quit
```

Verify that you can execute the read commands of the **ospf** feature.

```
[Switch] display ospf

          OSPF Process 1 with Router ID 192.168.1.50
                  OSPF Protocol Information

     RouterID: 192.168.1.50    Router type:
    Route tag: 0
    Multi-VPN-Instance is not enabled
    Ext-community type: Domain ID 0x5, Route Type 0x306, Router ID 0x107
    Domain ID: 0.0.0.0
    Opaque capable
    ISPF is enabled
    SPF-schedule-interval: 5 50 200
    LSA generation interval: 5 50 200
    LSA arrival interval: 1000
    Transmit pacing: Interval: 20 Count: 3
    Default ASE parameters: Metric: 1 Tag: 1 Type: 2
    Route preference: 10
    ASE route preference: 150
    SPF calculation count: 1
    RFC 1583 compatible
    Graceful restart interval: 120
    SNMP trap rate limit interval: 10  Count: 7
    Area count: 1   NSSA area count: 0
    ExChange/Loading neighbors: 0

    Area: 0.0.0.0          (MPLS TE  not enabled)
    Authtype: None    Area flag: Normal
    SPF scheduled count: 1
    ExChange/Loading neighbors: 0
```

Verify that you can execute the read and write commands of the **filesystem** feature. For example, specify the source IP address for outgoing FTP packets as 192.168.0.60.

```
[Switch] ftp client source ip 192.168.0.60
[Switch] quit
```

Verify that you cannot use the execute commands of the **filesystem** feature. For example, enter FTP client view.

```
<Switch> ftp
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface GigabitEthernet1/0/24
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write feature ospf
 rule 2 permit read write feature filesystem
#
local-user telnetuser class manage
password hash $h$6$3nDcf1enrif2H0W6$QUWsXcld9MjeCMWGlkU6qleuV3WqFFEE8i2TTSoFRL3
ENZ2ExkhXZZrRmOl3pblfbje6fim7vV+u5FbCif+SjA==
 service-type telnet
 authorization-attribute user-role role1
```

Example: Assigning access permissions to Telnet user through RADIUS server

Network configuration

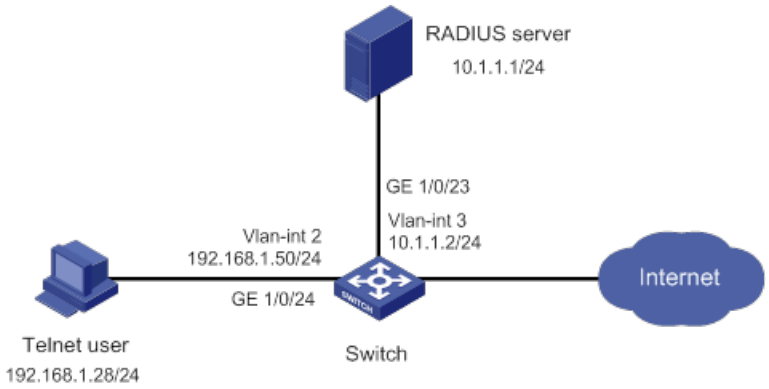
As shown in Figure 2, IMC is the RADIUS server, and the switch uses the RADIUS server to authenticate the Telnet user.

The server assigns the following access permissions to the Telnet user after the user passes authentication:

- Access all commands available in ISP domain view.
- Access the read and write commands of the ARP and RADIUS features.
- Create VLANs and access any commands available in VLAN view.
- Be blocked from all VLANs except VLANs 10 to 20.
- Access interface view to execute any commands available in interface view.
- Be blocked from all interfaces except GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

Add a user account named **telnetuser@bbb** on the server for the Telnet user, and specify a password for the account.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Add the ARP and RADIUS features to a feature group, so you can manage the features in a centralized manner.
- Create a user role and configure user role rules and resource access policies on the switch, so the user role can have the required access permissions.
- Specify the user role in the Telnet user account on the server, so the server can assign the user role to the Telnet user after the user passes authentication.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx

Hardware	Software version
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

Hardware	Software version
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure RBAC for remote AAA users, follow these guidelines:

- An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- Because RADIUS user authorization information is piggybacked in authentication responses, the authentication and authorization methods must use the same RADIUS scheme.
- You can create multiple rules for a user role. Each rule is uniquely identified by the rule number. A user role can access all commands permitted by the user role rules.

- If two user-defined rules conflict, the rule with the higher number takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**

Procedures

Configuring the switch

1. Configure VLAN settings:

Create VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

Assign GigabitEthernet 1/0/24 (the interface connected to the Telnet user) to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/24
[Switch-GigabitEthernet1/0/24] port access vlan 2
[Switch-GigabitEthernet1/0/24] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.50 24
[Switch-Vlan-interface2] quit
```

Create VLAN 3.

```
[Switch] vlan 3
[Switch-vlan3] quit
```

Assign GigabitEthernet 1/0/23 (the interface connected to the RADIUS server) to VLAN 3.

```
[Switch] interface gigabitethernet 1/0/23
[Switch-GigabitEthernet1/0/23] port access vlan 3
[Switch-GigabitEthernet1/0/23] quit
```

Assign an IP address to VLAN-interface 3.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 24
[Switch-Vlan-interface3] quit
```

2. Configure the user login authentication method:

Enable Telnet server.

```
[Switch] telnet server enable
```

Enable scheme authentication on user lines VTY 0 through VTY 63.

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

3. Configure RADIUS scheme **rad**:

Create RADIUS scheme **rad** and enter RADIUS scheme view.

```
[Switch] radius scheme rad
```

Specify the primary RADIUS authentication server at 10.1.1.1.

```
[Switch-radius-rad] primary authentication 10.1.1.1
```

Specify the primary RADIUS accounting server at 10.1.1.1.

```
[Switch-radius-rad] primary accounting 10.1.1.1
```

Set the authentication shared key to **hello12345** in plain text for secure RADIUS communication.

```
[Switch-radius-rad] key authentication simple hello12345
```

Set the accounting shared key to **hello12345** in plain text for secure RADIUS communication.

```
[Switch-radius-rad] key accounting simple hello12345
[Switch-radius-rad] quit
```

4. Configure ISP domain **bbb**:

Create ISP domain **bbb** and enter ISP domain view.

```
[Switch] domain bbb
```

Configure authentication, authorization, and accounting methods for the login users in the ISP domain.

```
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login radius-scheme rad
[Switch-isp-bbb] quit
```

5. Configure feature group **fgroup1**:

Create feature group **fgroup1** and enter feature group view.

```
[Switch] role feature-group name fgroup1
```

Assign the ARP and RADIUS features to the feature group.

```
[Switch-featuregrp-fgroup1] feature arp
[Switch-featuregrp-fgroup1] feature radius
[Switch-featuregrp-fgroup1] quit
```

6. Configure user role **role1**:

Create user role **role1** and enter user role view.

```
[Switch] role name role1
```

Configure rule 1 to permit the user role to access all commands in ISP domain view.

```
[Switch-role-role1] rule 1 permit command system-view ; domain *
```

Configure rule 2 to permit the user role to access all read and write commands of the features in feature group **fgroup1**.

```
[Switch-role-role1] rule 2 permit read write feature-group fgroup1
```

Configure rule 3 to permit the user role to create VLANs.

```
[Switch-role-role1] rule 3 permit command system-view ; vlan *
```

Configure rule 4 to permit the user role to enter interface view and execute all commands available in interface view.

```
[Switch-role-role1] rule 4 permit command system-view ; interface *
```

Enter user role VLAN policy view, and permit the user role to access only VLANs 10 through 20.

```
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] permit vlan 10 to 20
[Switch-role-role1-vlanpolicy] quit
```

Enter user role interface policy view, and permit the user role to access only interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
[Switch-role-role1] interface policy deny
[Switch-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/3
```

```
[Switch-role-role1-ifpolicy] quit
[Switch-role-role1] quit
```

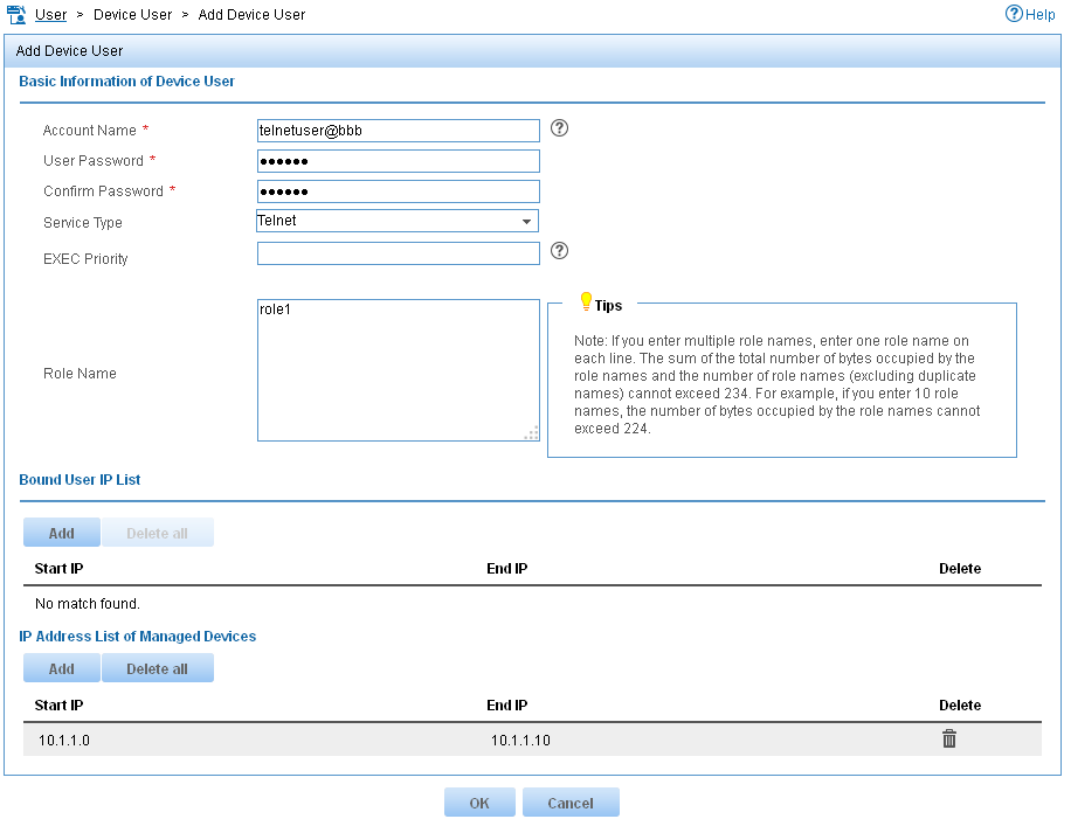
Configuring the RADIUS server

1. Add the switch to IMC as an access device:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.
   c. Click **Add**.

      The **Add Access Device** page appears.
   d. In the **Access Configuration** area, configure the following parameters:
      - Enter **1812** in the **Authentication Port** field, and enter **1813** in the **Accounting Port** field.
      - Enter **hello12345** in the **Shared Key** and **Confirm Shared Key** fields.
      - Select **Device Management Service** from the **Service Type** list.
      - Select a device type from the **Access Device Type** list.
      - Use the default values for other parameters.
   e. In the **Device List** area, click **Select** or **Add Manually** to add the switch (10.1.1.2) to IMC as an access device.
   f. Click **OK**.
2. Add a device management user:
   a. Click the **User** tab.
   b. From the navigation tree, select **Access User** > **Device User**.
   c. Click **Add**.

      The **Add Device User** page appears.
   d. In the **Basic Information of Device User** area, configure the following parameters, as shown in Figure 3:
      - Enter **telnetuser@bbb** in the **Account Name** field.
      - Enter a password in the **User Password** and **Confirm Password** fields.
      - Select **Telnet** from the **Service Type** list.
      - Enter **role1** in the **Role Name** field.

Figure 3 Adding a device management user



e. In the **IP Address List of Managed Devices** area, click **Add** to specify the IP address subnet in the range of 10.1.1.0 to 10.1.1.10.

f. Click **OK**.

Verifying the configuration

1. Display information about user role **role1**.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: deny
  Permitted VLANs: 10 to 20
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/1 to GigabitEthernet1/0/3
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit       command       system-view ; domain *
  2       permit RW-   feature-group fgroup1
  3       permit       command       system-view ; vlan *
  4       permit       command       system-view ; interface *
  R:Read W:Write X:Execute
```

2. Verify that you can Telnet to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

Verify that you can execute all commands available in ISP domain view.

```
<Switch> system-view
[Switch] domain abc
[Switch-isp-abc] authentication login radius-scheme abc
[Switch-isp-abc] quit
```

Verify that you can execute the read and write commands of the ARP and RADIUS features. For example, configure a RADIUS scheme.

```
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 2.2.2.2
[Switch-radius-rad] display radius scheme rad
[Switch-radius-rad] quit
```

Verify that you can access only VLANs 10 to 20. For example, create VLANs 10 and 30.

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 30
Permission denied.
```

Verify that you can access interfaces GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3. For example, configure GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] speed auto
[Switch-GigabitEthernet1/0/1] quit
```

Verify that you cannot access any interface except GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3. For example, enter the view of GigabitEthernet 1/0/6.

```
[Switch] interface gigabitethernet 1/0/6
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Vlan-interface3
```

```
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/23
 port access vlan 3
#
interface GigabitEthernet1/0/24
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
 key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
role feature-group name fgroup1
 feature arp
 feature radius
#
 role name role1
 rule 1 permit command system-view ; domain *
 rule 2 permit read write feature-group fgroup1
 rule 3 permit command system-view ; vlan *
 rule 4 permit command system-view ; interface *
 vlan policy deny
  permit vlan 10 to 20
 interface policy deny
  permit interface GigabitEthernet1/0/1 to GigabitEthernet1/0/3
#
```

Example: Configuring Telnet user to have access to specific commands in specific VPNs

Network configuration

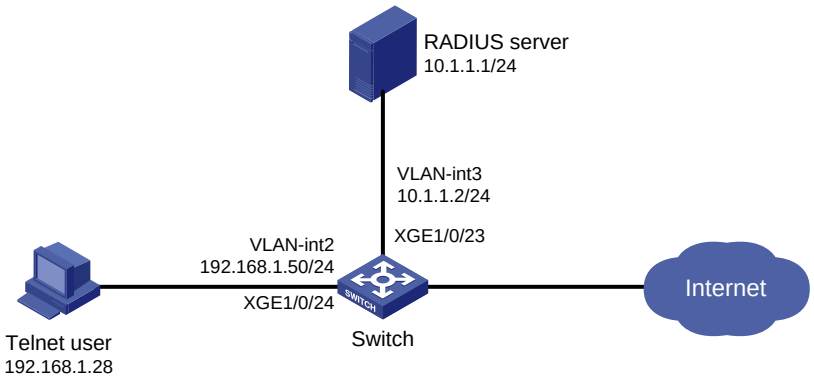
As shown in Figure 4, IMC is the RADIUS server, and the switch uses the RADIUS server to authenticate the Telnet user.

The server authorizes the following access permissions to the Telnet user after the user passes authentication:

- Access any commands available in the predefined feature group **L3**.
- Access any commands that start with the **`display`** keyword.
- Access only VPN instances **vpn1**, **vpn2**, and **vpn3**.

Add a user account named **telnetuser@bbb** on the server for the Telnet user, and specify a password for the account.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create a user role and configure user role rules and resource access policies on the switch, so the user role can have the required access permissions.
- Specify the user role in the Telnet user account on the server, so the server can assign the user role to the Telnet user after the user passes authentication.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx

Hardware	Software version
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure RBAC for remote AAA users, follow these restrictions and guidelines:

- An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- Because RADIUS user authorization information is piggybacked in authentication responses, the authentication and authorization methods must use the same RADIUS scheme.
- You can create multiple rules for a user role. Each rule is uniquely identified by the rule number. A user role can access all commands permitted by the user role rules.
- If two user-defined rules conflict, the rule with the higher number takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**

Procedures

Configuring the switch

1. Configure VLAN settings:

   # Create VLAN 2.

   ```
   <Switch> system-view
   [Switch] vlan 2
   [Switch-vlan2] quit
   ```

   # Assign GigabitEthernet 1/0/24 (the interface connected to the Telnet user) to VLAN 2.

   ```
   [Switch] interface gigabitethernet 1/0/24
   [Switch-GigabitEthernet1/0/24] port access vlan 2
   [Switch-GigabitEthernet1/0/24] quit
   ```

   # Assign an IP address to VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] ip address 192.168.1.50 24
   [Switch-Vlan-interface2] quit
   ```

   # Create VLAN 3.

   ```
   [Switch] vlan 3
   [Switch-vlan3] quit
   ```

   # Assign GigabitEthernet 1/0/23 (the interface connected to the RADIUS server) to VLAN 3.

   ```
   [Switch] interface gigabitethernet 1/0/23
   [Switch-GigabitEthernet1/0/23] port access vlan 3
   [Switch-GigabitEthernet1/0/23] quit
   ```

   # Assign an IP address to VLAN-interface 3.

   ```
   [Switch] interface vlan-interface 3
   [Switch-Vlan-interface3] ip address 10.1.1.2 24
   [Switch-Vlan-interface3] quit
   ```

2. Configure the user login authentication method:

   # Enable Telnet server.

   ```
   [Switch] telnet server enable
   ```

   # Enable scheme authentication on user lines VTY 0 through VTY 63.

   ```
   [Switch] line vty 0 63
   [Switch-line-vty0-63] authentication-mode scheme
   [Switch-line-vty0-63] quit
   ```

3. Configure RADIUS scheme **rad**:

   # Create RADIUS scheme **rad** and enter RADIUS scheme view.

   ```
   [Switch] radius scheme rad
   ```

   # Specify the primary RADIUS authentication server at 10.1.1.1.

   ```
   [Switch-radius-rad] primary authentication 10.1.1.1
   ```

   # Specify the primary RADIUS accounting server at 10.1.1.1.

   ```
   [Switch-radius-rad] primary accounting 10.1.1.1
   ```

   # Set the authentication shared key to **hello12345** in plain text for secure RADIUS communication.

   ```
   [Switch-radius-rad] key authentication simple hello12345
   ```

   # Set the accounting shared key to **hello12345** in plain text for secure RADIUS communication.

```
[Switch-radius-rad] key accounting simple hello12345
[Switch-radius-rad] quit
```

4. Configure ISP domain **bbb**:

   # Create ISP domain **bbb** and enter ISP domain view.

   ```
   [Switch] domain bbb
   ```

   # Specify the authentication, authorization, and accounting methods for the login users in the ISP domain.

   ```
   [Switch-isp-bbb] authentication login radius-scheme rad
   [Switch-isp-bbb] authorization login radius-scheme rad
   [Switch-isp-bbb] accounting login radius-scheme rad
   [Switch-isp-bbb] quit
   ```

5. Configure user role **role1**:

   # Create user role **role1** and enter user role view.

   ```
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to access all commands in the **L3** feature group.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L3
   ```

   # Configure rule 2 to permit the user role to access all commands that start with the **display** keyword.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

   # Enter user role VPN instance policy view, and configure the user role to have access only to VPN instances **vpn1**, **vpn2**, and **vpn3**.

   ```
   [Switch-role-role1] vpn policy deny
   [Switch-role-role1-vpnpolicy] permit vpn-instance vpn1 vpn2 vpn3
   [Switch-role-role1-vpnpolicy] quit
   [Switch-role-role1] quit
   ```

Configuring the RADIUS server

1. Add the switch to IMC as an access device:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.
   c. Click **Add**.

      The **Add Access Device** page appears.
   d. In the **Access Configuration** area, configure the following parameters:
      - Enter **1812** in the **Authentication Port** field, and enter **1813** in the **Accounting Port** field.
      - Enter **hello12345** in the **Shared Key** and **Confirm Shared Key** fields.
      - Select **Device Management Service** from the **Service Type** list.
      - Select a device type from the **Access Device Type** list.
      - Use the default values for other parameters.
   e. In the **Device List** area, click **Select** or **Add Manually** to add the switch (10.1.1.2) to IMC as an access device.
   f. Click **OK**.
2. Add a device management user:
   a. Click the **User** tab.
   b. From the navigation tree, select **Access User** > **Device User**.

c. Click **Add**.

   The **Add Device User** page appears.

d. In the **Basic Information of Device User** area, configure the following parameters, as shown in Figure 5:

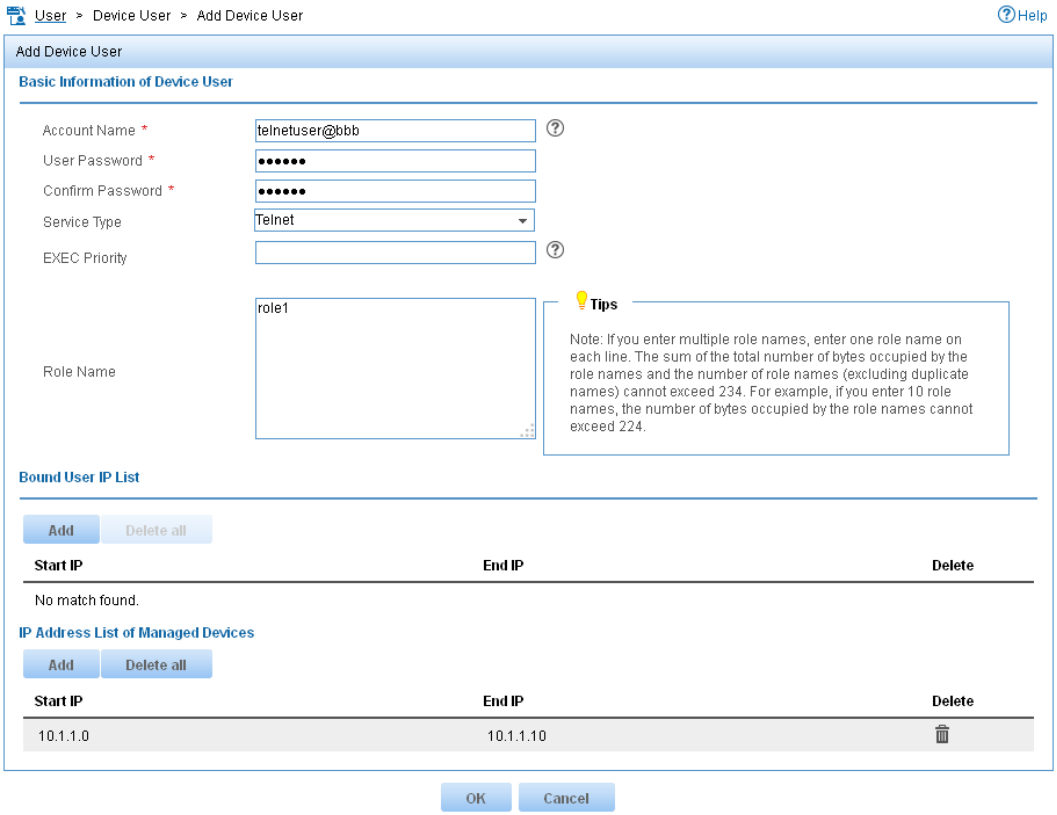
   – Enter **telnetuser@bbb** in the **Account Name** field.

   – Enter a password in the **User Password** and **Confirm Password** fields.

   – Select **Telnet** from the **Service Type** list.

   – Enter **role1** in the **Role Name** field.

Figure 5 Adding a device management user



e. In the **IP Address List of Managed Devices** area, click **Add** to specify the IP address subnet in the range of 10.1.1.0 to 10.1.1.10.

f. Click **OK**.

Verifying the configuration

1. Display information about user role **role1**.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: deny
  Permitted VPN instances: vpn1, vpn2, vpn3
  ----------------------------------------------------------------------
```

```
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------
  1       permit RWX   feature-group L3
  2       permit       command       display *
  R:Read W:Write X:Execute
```

2. Use the **display role feature-group** command to display the features in feature group **L3**. (Details not shown.)
3. Verify that you can Telnet to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can execute all commands available in the **L3** feature group. For example, create VPN instance **vpn1** and configure a RD for the VPN instance.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
[Switch-vpn-instance-vpn1] route-distinguisher 22:1
[Switch-vpn-instance-vpn1] display this
#
ip vpn-instance vpn1
 route-distinguisher 22:1
#
return
[Switch-vpn-instance-vpn1] quit
```

   # Verify that you cannot access any VPN instance except **vpn1**, **vpn2**, and **vpn3**. For example, create VPN instance **vpn5**.

```
[Switch] ip vpn-instance vpn5
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/23
port access vlan 3
#
interface GigabitEthernet1/0/24
port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
 key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 vpn-instance policy deny
  permit vpn-instance vpn1
  permit vpn-instance vpn2
  permit vpn-instance vpn3
#
```

Example: Changing user access permissions by assigning new user roles

Network configuration

As shown in Figure 6, add two user accounts **telnetuser1** and **telnetuser2** on the switch for Telnet user 1 and Telnet user 2, respectively. Set both the users' passwords to **hello12345** in plain text.

Configure the switch to meet the following requirements:

- The Telnet users are authenticated on the switch in ISP domain **bbb**.
- User role **role1** is assigned to the Telnet users after they pass authentication.

User role **role1** has the following access permissions:

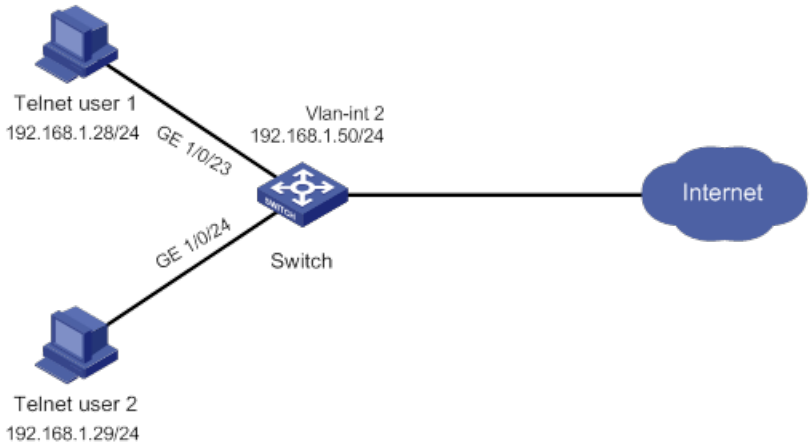
- Access any commands that start with the **`display`** keyword.
- Create VLANs.
- Access only VLANs 10 to 15.

- Access only interface GigabitEthernet 1/0/1.

Telnet user 1 requires adding the following access permissions:

- Access VLANs 16 to 20.
- Access interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

Figure 6 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create a user role and configure user role rules and resource access policies, so the user role can have the additional access permissions of Telnet user 1.
- Assign the user role to Telnet user 1, so the user can have the additional access permissions at the next login.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx

Hardware	Software version
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx

Hardware	Software version
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you assign another user role to a user, follow these restrictions and guidelines:

- You can create multiple rules for a user role. Each rule is uniquely identified by the rule number. A user role can access all commands permitted by the user role rules.
- If two user-defined rules conflict, the rule with the higher number takes effect. For example, the user role can use the **`tracert`** command but not the **`ping`** command if the user role contains rules configured by using the following commands:
  - **`rule 1 permit command ping`**
  - **`rule 2 permit command tracert`**
  - **`rule 3 deny command ping`**
- You can assign multiple user roles to a user. The user can use the collection of items and resources accessible to any user role assigned to it.
- If you assign a new user role to a user when the user is online, the assignment does not take effect on the user at the current login. The user obtains the user role the next time it logs in to the switch.

Procedures

Assigning user role role1 to the Telnet users

1. Configure VLAN settings:

   # Create VLAN 2.

   ```
   <Switch> system-view
   [Switch] vlan 2
   [Switch-vlan2] quit
   ```

   # Assign interfaces GigabitEthernet 1/0/23 and GigabitEthernet 1/0/24 (the interfaces connected to the Telnet users) to VLAN 2.

   ```
   [Switch] interface gigabitethernet 1/0/23
   [Switch-GigabitEthernet1/0/23] port access vlan 2
   [Switch-GigabitEthernet1/0/23] quit
   [Switch] interface gigabitethernet 1/0/24
   [Switch-GigabitEthernet1/0/24] port access vlan 2
   [Switch-GigabitEthernet1/0/24] quit
   ```

   # Assign an IP address to VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] ip address 192.168.1.50 24
   [Switch-Vlan-interface2] quit
   ```

2. Configure the user login authentication method:

   # Enable Telnet server.

   ```
   [Switch] telnet server enable
   ```

   # Enable scheme authentication on user lines VTY 0 through VTY 63.

   ```
   [Switch] line vty 0 63
   [Switch-line-vty0-63] authentication-mode scheme
   [Switch-line-vty0-63] quit
   ```

3. Configure ISP domain bbb:

   # Create ISP domain **bbb** and enter ISP domain view.

   ```
   [Switch] domain bbb
   ```

   # Configure the authentication and authorization methods for the login users in the ISP domain.

   ```
   [Switch-isp-bbb] authentication login local
   [Switch-isp-bbb] authorization login local
   [Switch-isp-bbb] quit
   ```

4. Configure device management users **telnetuser1** and **telnetuser2**:

   # Create device management user **telnetuser1** and enter local user view.

   ```
   [Switch] local-user telnetuser1 class manage
   ```

   # Set the password to **hello12345** in plain text.

   ```
   [Switch-luser-manage-telnetuser1] password simple hello12345
   ```

   # Specify the service type as Telnet.

   ```
   [Switch-luser-manage-telnetuser1] service-type telnet
   [Switch-luser-manage-telnetuser1] quit
   ```

   # Create device management user **telnetuser2** and enter local user view.

   ```
   [Switch] local-user telnetuser2 class manage
   ```

   # Set the password to **hello12345** in plain text.

```
[Switch-luser-manage-telnetuser2] password simple hello12345
```

Specify the service type as Telnet.

```
[Switch-luser-manage-telnetuser2] service-type telnet
[Switch-luser-manage-telnetuser2] quit
```

5. Configure user role **role1**:

Create user role **role1** and enter user role view.

```
[Switch] role name role1
```

Configure rule 1 to permit the user role to access all commands that start with the **display** keyword.

```
[Switch-role-role1] rule 1 permit command display *
```

Configure rule 2 to permit the user role to access VLAN view.

```
[Switch-role-role1] rule 2 permit command system-view ; vlan *
```

Configure rule 3 to permit the user role to enter interface view and execute all commands available in interface view.

```
[Switch-role-role1] rule 3 permit command system-view ; interface *
```

Enter user role VLAN policy view, and allow the user role to access only VLANs 10 to 15.

```
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] permit vlan 10 to 15
[Switch-role-role1-vlanpolicy] quit
```

Enter user role interface policy view, and allow the user role to access only interface GigabitEthernet 1/0/1.

```
[Switch-role-role1] interface policy deny
[Switch-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1
[Switch-role-role1-ifpolicy] quit
[Switch-role-role1] quit
```

6. Assign user role **role1** to the device management users:

Enter the view of **telnetuser1**.

```
[Switch] local-user telnetuser1 class manage
```

Assign user role **role1** to **telnetuser1**.

```
[Switch-luser-manage-telnetuser1] authorization-attribute user-role role1
```

Remove the default user role **network-operator** from **telnetuser1**.

```
[Switch-luser-manage-telnetuser1] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser1] quit
```

Enter the view of **telnetuser2**.

```
[Switch] local-user telnetuser2 class manage
```

Assign user role **role1** to **telnetuser2**.

```
[Switch-luser-manage-telnetuser2] authorization-attribute user-role role1
```

Remove the default user role **network-operator** from **telnetuser2**.

```
[Switch-luser-manage-telnetuser2] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser2] quit
```

Verifying the access permissions of user role role1

1. Display information about user role **role1**.

```
[Switch] display role name role1
Role: role1
```

```
  Description:
  VLAN policy: deny
  Permitted VLANs: 10 to 15
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/1
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  1       permit       command       display *
  2       permit       command       system-view ; vlan *
  3       permit       command       system-view ; interface *
  R:Read W:Write X:Execute
```

2. Verify that you can Telnet to the switch. This example uses the user account **telnetuser1@bbb**.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser1@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Switch>
```

3. Verify that you have the access permissions of user role **role1**:

   # Verify that you can configure VLANs 10 to 15. For example, create VLAN 15.

```
<Switch> system-view
[Switch] vlan 15
[Switch-vlan15] quit
```

   # Verify that you cannot access any other VLAN except VLANs 10 to 15. For example, create VLAN 20.

```
[Switch] vlan 20
Permission denied.
```

   # Verify that you can access interface GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] speed auto
[Switch-GigabitEthernet1/0/1] quit
```

Assigning user role role2 to Telnet user 1

1. Configure user role **role2**:

   # Create user role **role2** and enter user role view.

```
[Switch] role name role2
```

   # Configure rule 1 to permit the user role to enter interface view and execute all commands available in interface view.

```
[Switch-role-role2] rule 1 permit command system-view ; interface *
```

   # Enter user role VLAN policy view, and allow the user role to access only VLANs 16 to 20.

```
[Switch-role-role2] vlan policy deny
[Switch-role-role2-vlanpolicy] permit vlan 16 to 20
[Switch-role-role2-vlanpolicy] quit
```

Enter user role interface policy view, and allow the user role to access only interfaces GigabitEthernet 1/0/2 to GigabitEthernet 1/0/3.

```
[Switch-role-role2] interface policy deny
[Switch-role-role2-ifpolicy] permit interface gigabitethernet 1/0/2 to
gigabitethernet 1/0/3
[Switch-role-role2-ifpolicy] quit
[Switch-role-role2] quit
```

2. Assign user role **role2** to **telnetuser1**:

Enter the view of **telnetuser1**.

```
[Switch] local-user telnetuser1 class manage
```

Assign user role **role2** to **telnetuser1**.

```
[Switch-luser-manage-telnetuser1] authorization-attribute user-role role2
[Switch-luser-manage-telnetuser1] quit
```

Verifying the configuration

1. Display information about user role **role2**.

```
[Switch] display role name role2
Role: role2
  Description:
  VLAN policy: deny
  Permitted VLANs: 16 to 20
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/2 to GigabitEthernet1/0/3
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit       command       system-view ; interface *
  R:Read W:Write X:Execute
```

2. Verify that you can Telnet to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser1@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

3. Verify that you have the access permissions of user role **role2**:

Verify that you can access VLANs 16 to 20. For example, create VLAN 16.

```
<Switch> system-view
[Switch] vlan 16
```

```
[Switch-vlan16] quit
```

Verify that you can access interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. For example, configure GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] speed auto
[Switch-GigabitEthernet1/0/2] quit
```

Verify that you cannot access any other interface except interfaces GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3. For example, enter the view of GigabitEthernet 1/0/5.

```
[Switch] interface gigabitethernet 1/0/5
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface GigabitEthernet1/0/23
port access vlan 2
#
interface GigabitEthernet1/0/24
port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit command display *
 rule 2 permit command system-view ; vlan *
 rule 3 permit command system-view ; interface *
 vlan policy deny
  permit vlan 10 to 15
 interface policy deny
  permit interface GigabitEthernet1/0/1
#
role name role2
 rule 1 permit command system-view ; interface *
 vlan policy deny
  permit vlan 16 to 20
```

```
 interface policy deny
  permit interface GigabitEthernet1/0/2 to GigabitEthernet1/0/3
#
 local-user telnetuser1 class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
 authorization-attribute user-role role2
#
 local-user telnetuser2 class manage
 password hash TPcgyTQJZShe$h$6$vaSj2xKc8yFiNdfQ$Jzb3PXo2lt4jk KSZqJUVhjP634Wol/
Qx8TLU748IHoeui0w5n/XRzpNqbNnpxikym39gGJCwYw==
 service-type telnet
 authorization-attribute user-role role1
#
```

Example: Configuring temporary user role authorization

Network configuration

As shown in Figure 7, the switch performs local AAA authentication for the Telnet user. It assigns user role **role1** to the Telnet user after the user passes authentication.

The switch performs local-only authentication for the Telnet user to obtain the user role **role2** or **network-operator** for temporary authorization.

User role **role1** has the following access permissions:

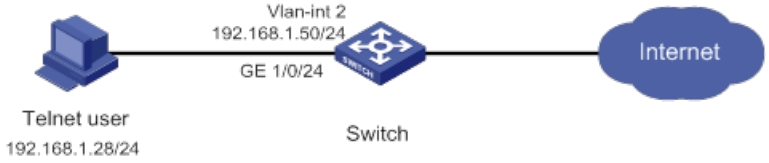
- Access any commands available in the **L3** feature group.
- Access any commands that start with the **display** keyword.
- Access any commands that start with the **super** keyword.
- Access any interfaces, VLANs, and VPNs.

User role **role2** has the following access permissions:

- Access any commands available in the **L2** feature group.
- Access any interfaces, VLANs, and VPNs.

Add a user account named **telnetuser** on the switch for the Telnet user, set the password to **hello12345** in plain text.

Figure 7 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create user roles **role1** and **role2**, and configure user role rules and resource access policies, so the user roles can have the required access permissions.
- Assign user role **role1** to the Telnet user, so the user can obtain the user role after it passes authentication.
- Configure user role authentication settings for **role2** and **network-operator**, so the Telnet user can obtain the user roles for temporary authorization.
- For security purposes, configure different authentication passwords for the user roles **role2** and **network-operator**.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx

Hardware	Software version
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure temporary user role authorization, follow these restrictions and guidelines:

- An ISP domain cannot be deleted when it is the default ISP domain. Before you use the **undo domain** command, change the domain to a non-default ISP domain by using the **undo domain default enable** command.
- You can create multiple rules for a user role. Each rule is uniquely identified by the rule number. A user role can access all commands permitted by the user role rules.
- If two user-defined rules conflict, the rule with the higher number takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**
- Temporary user role authorization is effective only on the current login. This feature does not change the user role settings in the user account that you have been logged in with. The next time you are logged in with the user account, the original user role settings take effect.

Procedures

1. Configure VLAN settings:

   # Create VLAN 2.

   ```
   <Switch> system-view
   [Switch] vlan 2
   [Switch-vlan2] quit
   ```

   # Assign GigabitEthernet 1/0/24 (the interface connected to the Telnet user) to VLAN 2.

   ```
   [Switch] interface gigabitethernet 1/0/24
   [Switch-GigabitEthernet1/0/24] port access vlan 2
   [Switch-GigabitEthernet1/0/24] quit
   ```

   # Assign an IP address to VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] ip address 192.168.1.50 24
   [Switch-Vlan-interface2] quit
   ```

2. Configure the user login authentication method:

   # Enable Telnet server.

   ```
   [Switch] telnet server enable
   ```

   # Enable scheme authentication on user lines VTY 0 through VTY 63.

   ```
   [Switch] line vty 0 63
   [Switch-line-vty0-63] authentication-mode scheme
   [Switch-line-vty0-63] quit
   ```

3. Configure ISP domain **bbb**:

   # Create ISP domain **bbb** and enter ISP domain view.

   ```
   [Switch] domain bbb
   ```

   # Configure the authentication and authorization methods for the login users in the ISP domain.

   ```
   [Switch-isp-bbb] authentication login local
   [Switch-isp-bbb] authorization login local
   [Switch-isp-bbb] quit
   ```

4. Configure device management user **telnetuser**:

   # Create device management user **telnetuser** and enter local user view.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Set the user password to **hello12345** in plain text.

   ```
   [Switch-luser-manage-telnetuser] password simple hello12345
   ```

   # Specify the service type as Telnet.

   ```
   [Switch-luser-manage-telnetuser] service-type telnet
   [Switch-luser-manage-telnetuser] quit
   ```

5. Configure user role **role1**:

   # Create user role **role1** and enter user role view.

   ```
   [Switch] role name role1
   ```

   # Configure rule 1 to permit the user role to access all commands of the **L3** feature group.

   ```
   [Switch-role-role1] rule 1 permit execute read write feature-group L3
   ```

   # Configure rule 2 to permit the user role to access all commands that start with the **display** keyword.

   ```
   [Switch-role-role1] rule 2 permit command display *
   ```

   # Configure rule 3 to permit the user role to access all commands that start with the **super** keyword.

   ```
   [Switch-role-role1] rule 3 permit command super *
   [Switch-role-role1] quit
   ```

6. Configure user role **role2**:

   # Create user role **role2** and enter user role view.

   ```
   [Switch] role name role2
   ```

   # Configure rule 1 to permit the user role to access all commands of the **L2** feature group.

   ```
   [Switch-role-role2] rule 1 permit execute read write feature-group L2
   [Switch-role-role2] quit
   ```

7. Authorize user role **role1** to device management user **telnetuser**:

   # Enter the view of the device management user.

   ```
   [Switch] local-user telnetuser class manage
   ```

   # Authorize user role **role1** to the user.

   ```
   [Switch-luser-manage-telnetuser] authorization-attribute user-role role1
   ```

   # Remove the default user role **network-operator** from the user.

```
[Switch-luser-manage-telnetuser] undo authorization-attribute user-role
network-operator
[Switch-luser-manage-telnetuser] quit
```

8. Configure temporary user role authorization:

Enable local-only authentication for temporary user role authorization.

```
[Switch] super authentication-mode local
```

Set the local authentication password to **123456TESTplat&!** in plain text for user role **role2**.

```
[Switch] super password role role2 simple 123456TESTplat&!
```

Set the local authentication password to **987654TESTplat&!** in plain text for user role **network-operator**.

```
[Switch] super password role network-operator simple 987654TESTplat&!
```

Verifying the configuration

1. Verify that the user roles are correctly configured:

Display information about user role **role1**.

```
[Switch] display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L3
  2       permit       command       display *
  3       permit       command       super *
  R:Read W:Write X:Execute
```

Display information about user role **role2**.

```
[Switch] display role name role2
Role: role2
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L2
  R:Read W:Write X:Execute
```

Display information about user role **network-operator**.

```
[Switch] display role name network-operator
Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
```

```
VPN instance policy: permit (default)
-------------------------------------------------------------------
Rule    Perm   Type  Scope         Entity
-------------------------------------------------------------------
sys-1   permit       command       display *
sys-2   permit       command       xml
sys-3   permit       command       system-view ; probe ; display *
sys-4   deny         command       display history-command all
sys-5   deny         command       display exception *
sys-6   deny         command       display cpu-usage configuration
                                   *
sys-7   deny         command       display kernel exception *
sys-8   deny         command       display kernel deadloop *
sys-9   deny         command       display kernel starvation *
sys-10  deny         command       display kernel reboot *
sys-13  permit       command       system-view ; local-user *
sys-16  permit R--   web-menu      -
sys-17  permit RW-   web-menu      m_device/m_maintenance/
                                   m_changepassword
sys-18  permit R--   xml-element   -
sys-19  deny         command       display security-logfile summary
sys-20  deny         command       display security-logfile buffer
sys-21  deny         command       system-view ; info-center
                                   security-logfile directory *
sys-22  deny         command       security-logfile save
sys-23  deny         command       system-view ; local-user-import
                                   *
sys-24  deny         command       system-view ; local-user-export
                                   *
sys-25  permit R--   oid           1
R:Read W:Write X:Execute
```

2. Use the **`display role feature-group`** command to display the features in the **L2** and **L3** feature groups. (Details not shown.)
3. Verify that you can Telnet to the switch.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Switch>
```

4. Verify that you have the access permissions of user role **role1**:

   # Verify that you can access all commands in the **L3** feature group. For example, create VPN **vpn1**.

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
```

```
[Switch-vpn-instance-vpn1] quit
```

Verify that you can use all commands that start with the **display** keyword. For example, display the system time and date.

```
[Switch] display clock
13:53:24.357 test Sat 01/01/2018
Time Zone : test add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
[Switch] quit
```

5. Verify that you can obtain the authorization of user role **role2** without reconnecting to the switch:

Obtain the user role **role2**.

```
<Switch> super role2
Password:
User privilege role is role2, and only those commands that authorized to the role can
be used.
<Switch>
```

Verify that you can use all commands in the **L2** feature group. For example, create VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] quit
```

Verify that you cannot use the commands of any features except the features in the **L2** feature group. For example, obtain the user role **network-operator** for temporary authorization.

```
<Switch> super network-operator
Permission denied.
```

Verify that you cannot use the commands that start with the **display** keyword. For example, display the system date and time.

```
<Switch> display clock
Permission denied.
```

6. Disconnect from the switch, and Telnet to the switch again.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Switch>
```

7. Verify that you can obtain the **network-operator** user role.

```
<Switch> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized
 to the role can be used.
<Switch>
```

Configuration files

```
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface GigabitEthernet1/0/24
port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 super password role role2 hash $h$6$D0kjHFktkktzgR5g$e673xFnIcKytCj6EDAw+pvwgh3
/ung3WNWHnrUTnXT862B+s7PaLfKTdil8ef71RBOvuJvPAZHjiLjrMPyWHQw==
 super password role network-operator hash $h$6$3s5KMmscn9hJ6gPx$IcxbNjUc8u4yxwR
m87b/Jki8BoPAxw/s5bEcPQjQj/cbbXwTVcnQGL91WOd7ssO2rX/wKzfyzAO5VhBTn9Q4zQ==
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 rule 3 permit command super *
#
role name role2
 rule 1 permit read write execute feature-group L2
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

Example: Assigning ACL and QoS access permissions to Telnet users

Network configuration

As shown in Figure 8, the core switch is an HPE xxxx switch, and IMC is the RADIUS server. Users in Department A are in VLANs 100 to 199, and users in Department B are in VLANs 200 to 299. Users in the two departments cannot reach each other at Layer 2.

Add Telnet user accounts **admin-departA@bbb** and **admin-departB@bbb** on the RADIUS server for the network administrators in Department A and Department B, respectively.

The core switch uses the RADIUS server to authenticate the network administrators in ISP domain **bbb**.

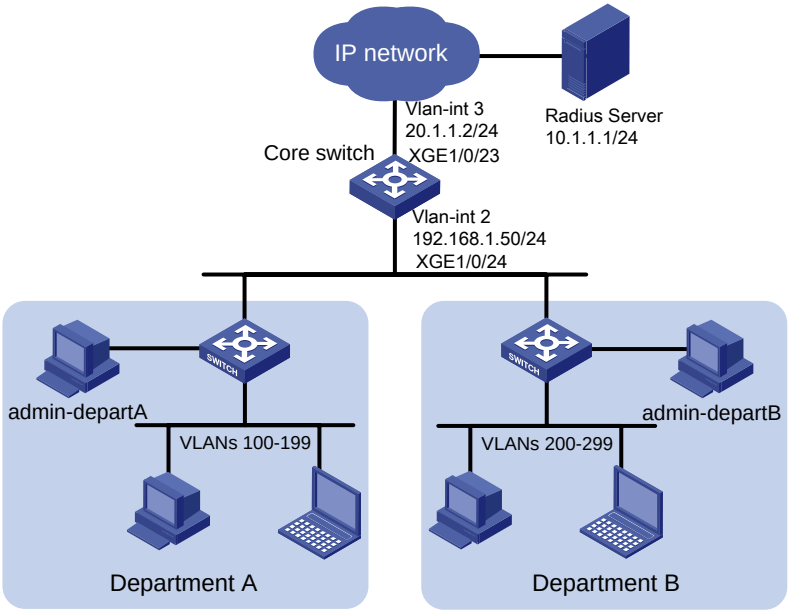
The server assigns the following access permissions to **admin-departA** after it passes authentication:

- Access any commands of the ACL and QoS features.
- Access VLANs 100 to 199.
- Be blocked from all interfaces and VPNs.

The server assigns the following access permissions to **admin-departB** after it passes authentication:

- Access any commands of the ACL and QoS features.
- Access VLANs 200 to 299.
- Be blocked from all interfaces and VPNs.

Figure 8 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create a user role and configure user role rules and resource access policies on the core switch for each administrator, so the user roles can have the required access permissions.
- Specify the correct user role in each Telnet user account on the server, so the server can assign the correct user role to each administrator.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and	Release 11xx

Hardware	Software version
S5500V3-48P-SI)	
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

Hardware	Software version
IE4300-M switch series IE4320 switch series	
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

Because RADIUS user authorization information is piggybacked in authentication responses, the authentication and authorization methods must use the same RADIUS scheme.

Procedures

Configuring the core switch

1. Configure VLAN settings:

Create VLAN 2.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

Assign GigabitEthernet 1/0/24 (the interface connected to the Telnet users) to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/24
[Switch-GigabitEthernet1/0/24] port access vlan 2
[Switch-GigabitEthernet1/0/24] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.50 24
[Switch-Vlan-interface2] quit
```

Create VLAN 3.

```
[Switch] vlan 3
[Switch-vlan3] quit
```

Assign GigabitEthernet 1/0/23 (the interface connected to the RADIUS server) to VLAN 3.

```
[Switch] interface gigabitethernet 1/0/23
[Switch-GigabitEthernet1/0/23] port access vlan 3
[Switch-GigabitEthernet1/0/23] quit
```

Assign an IP address to VLAN-interface 3.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 20.1.1.2 24
[Switch-Vlan-interface3] quit
```

2. Configure the user login authentication method:

Enable Telnet server.

```
[Switch] telnet server enable
```

Enable scheme authentication on user lines VTY 0 through VTY 63.

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
```

```
[Switch-line-vty0-63] quit
```

3. Configure RADIUS scheme **rad**:

   # Create RADIUS scheme **rad** and enter RADIUS scheme view.

   ```
   [Switch] radius scheme rad
   ```

   # Specify the primary RADIUS authentication server at 10.1.1.1.

   ```
   [Switch-radius-rad] primary authentication 10.1.1.1
   ```

   # Specify the primary RADIUS accounting server at 10.1.1.1.

   ```
   [Switch-radius-rad] primary accounting 10.1.1.1
   ```

   # Set the authentication shared key to **hello12345** in plain text for secure RADIUS communication.

   ```
   [Switch-radius-rad] key authentication simple hello12345
   ```

   # Set the accounting shared key to **hello12345** in plain text for secure RADIUS communication.

   ```
   [Switch-radius-rad] key accounting simple hello12345
   [Switch-radius-rad] quit
   ```

4. Configure ISP domain **bbb**:

   # Create ISP domain **bbb** and enter ISP domain view.

   ```
   [Switch] domain bbb
   ```

   # Configure authentication, authorization, and accounting methods for the login users in the ISP domain.

   ```
   [Switch-isp-bbb] authentication login radius-scheme rad
   [Switch-isp-bbb] authorization login radius-scheme rad
   [Switch-isp-bbb] accounting login radius-scheme rad
   [Switch-isp-bbb] quit
   ```

5. Configure user role **departA-resource**:

   # Create user role **departA-resource** and enter user role view.

   ```
   [Switch] role name departA-resource
   ```

   # Configure rule 1 to permit the user role to access all commands of the QoS feature.

   ```
   [Switch-role-departA-resource] rule 1 permit read write execute feature qos
   ```

   # Configure rule 2 to permit the user role to access all commands of the ACL feature.

   ```
   [Switch-role-departA-resource] rule 2 permit read write execute feature acl
   ```

   # Enter user role VLAN policy view, and permit the user role to access only VLANs 100 to 199.

   ```
   [Switch-role-departA-resource] vlan policy deny
   [Switch-role-departA-resource-vlanpolicy] permit vlan 100 to 199
   [Switch-role-departA-resource-vlanpolicy] quit
   ```

   # Deny the user role to access any interface and VPN.

   ```
   [Switch-role-departA-resource] interface policy deny
   [Switch-role-departA-resource-ifpolicy] quit
   [Switch-role-departA-resource] vpn policy deny
   [Switch-role-departA-resource-vpnpolicy] quit
   [Switch-role-departA-resource] quit
   ```

6. Configure user role **departB-resource**:

   # Create user role **departB-resource** and enter user role view.

   ```
   [Switch] role name departB-resource
   ```

   # Configure rule 1 to permit the user role to access all commands of the QoS feature.

   ```
   [Switch-role-departB-resource] rule 1 permit read write execute feature qos
   ```

   # Configure rule 2 to permit the user role to access all commands of the ACL feature.

   ```
   [Switch-role-departB-resource] rule 2 permit read write execute feature acl
   ```

Enter user role VLAN policy view, and permit the user role to access only VLANs 200 to 299.

```
[Switch-role-departB-resource] vlan policy deny
[Switch-role-departB-resource-vlanpolicy] permit vlan 200 to 299
[Switch-role-departB-resource-vlanpolicy] quit
```

Deny the user role to access any interface and VPN.

```
[Switch-role-departB-resource] interface policy deny
[Switch-role-departB-resource-ifpolicy] quit
[Switch-role-departB-resource] vpn policy deny
[Switch-role-departB-resource-vpnpolicy] quit
[Switch-role-departB-resource] quit
```

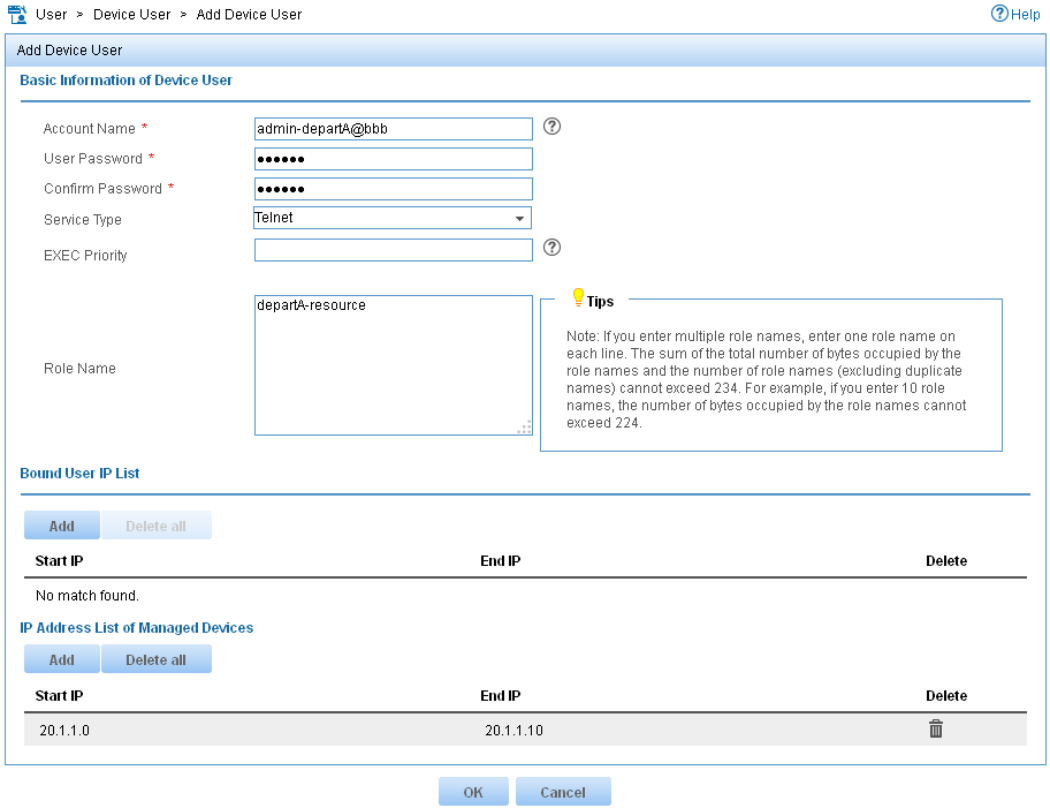
Configuring the RADIUS server

1. Add the core switch to IMC as an access device:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.
   c. Click **Add**.

      The **Add Access Device** page appears.
   d. In the **Access Configuration** area, configure the following parameters:
      - Enter **1812** in the **Authentication Port** field, and enter **1813** in the **Accounting Port** field.
      - Enter **hello12345** in the **Shared Key** and **Confirm Shared Key** fields.
      - Select **Device Management Service** from the **Service Type** list.
      - Select a device type from the **Access Device Type** list.
      - Use the default values for other parameters.
   e. In the **Device List** area, click **Select** or **Add Manually** to add the core switch (20.1.1.2) to IMC as an access device.
   f. Click **OK**.
2. Add a device management user:
   a. Click the **User** tab.
   b. From the navigation tree, select **Access User** > **Device User**.
   c. Click **Add**.

      The **Add Device User** page appears.
   d. In the **Basic Information of Device User** area, configure the following parameters, as shown in Figure 9:
      - Enter **admin-departA@bbb** in the **Account Name** field.
      - Enter a password in the **User Password** and **Confirm Password** fields.
      - Select **Telnet** from the **Service Type** list.
      - Enter **departA-resource** in the **Role Name** field.

Figure 9 Adding a device management user



e. In the **IP Address List of Managed Devices** area, click **Add** to specify the IP address subnet in the range of 20.1.1.0 to 20.1.1.10.

f. Click **OK**.

The device user list displays the added user.

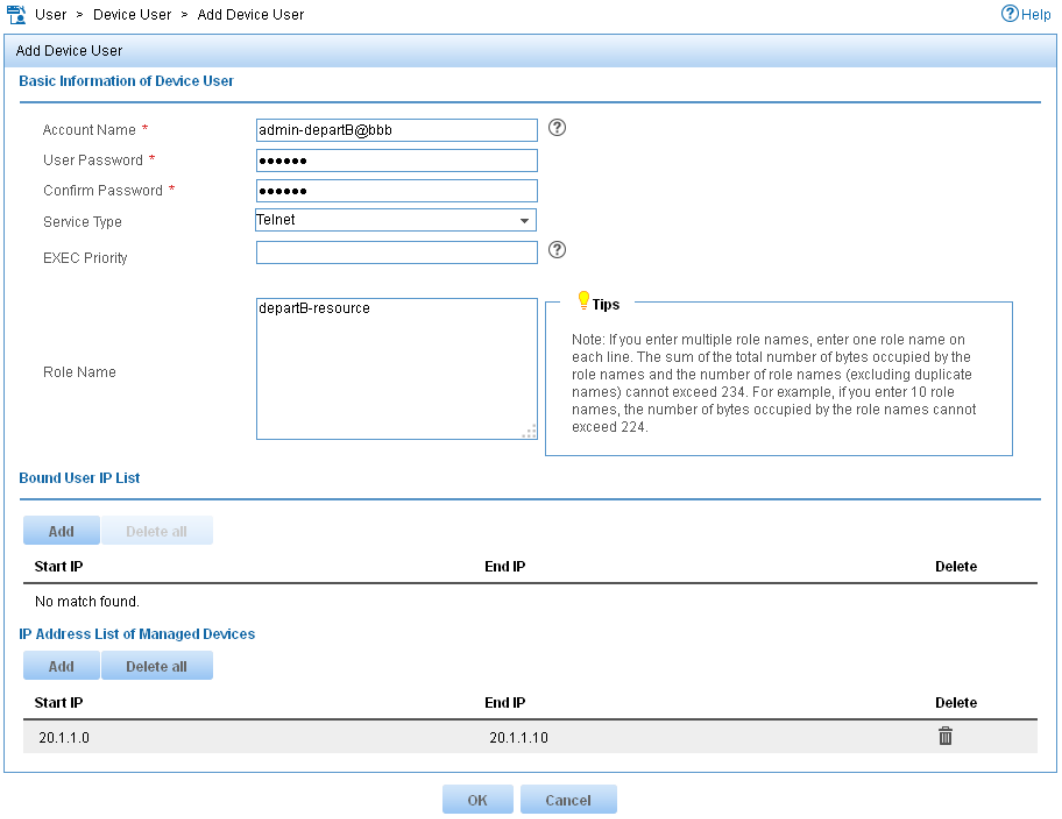
g. Click **Add**.

The **Add Device User** page appears.

h. In the **Basic Information of Device User** area, configure the following parameters, as shown in Figure 10:

- Enter **admin-departB@bbb** in the **Account Name** field.
- Enter a password in the **User Password** and **Confirm Password** fields.
- Select **Telnet** from the **Service Type** list.
- Enter **departB-resource** in the **Role Name** field.

Figure 10 Adding a device management user



i. In the **IP Address List of Managed Devices** area, click **Add** to specify the IP address subnet in the range of 20.1.1.0 to 20.1.1.10.

j. Click **OK**.

Verifying the configuration

1. Verify that the user roles are correctly configured:

   # Display information about user role **departA-resource**.

```
[Switch] display role name departA-resource
Role: departA-resource
  Description:
  VLAN policy: deny
  Permitted VLANs: 100 to 199
  Interface policy: deny
  VPN instance policy: deny
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature       qos
  2       permit RWX   feature       acl
  R:Read W:Write X:Execute
```

   # Display information about user role **departB-resource**.

```
[Switch] display role name departB-resource
Role: departB-resource
```

```
  Description:
  VLAN policy: deny
  Permitted VLANs: 200 to 299
  Interface policy: deny
  VPN instance policy: deny
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature       qos
  2       permit RWX   feature       acl
  R:Read W:Write X:Execute
```

2. Verify that you can Telnet to the core switch by using the account **admin-departA@bbb** from Department A:

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: admin-departA@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Switch>
```

3. Verify that you have the access permission of user role **departA-resource**:

a. Verify that you can use all commands of the QoS and ACL features:

Create IPv4 advanced ACL 3000 and enter ACL view.

```
<Switch> system-view
[Switch] acl number 3000
```

Create an IPv4 advanced ACL rule to permit outbound FTP packets.

```
[Switch-acl-ipv4-adv-3000] rule permit tcp destination-port eq ftp-data
[Switch-acl-ipv4-adv-3000] quit
```

Create traffic class **1** and enter traffic class view.

```
[Switch] traffic classifier 1
```

Define a match criterion for traffic class **1** to match the advanced ACL 3000.

```
[Switch-classifier-1] if-match acl 3000
[Switch-classifier-1] quit
```

Create traffic behavior **1** and enter traffic behavior view.

```
[Switch] traffic behavior 1
```

Set the CIR of the CAR action to 2000 kbps.

```
[Switch-behavior-1] car cir 2000
[Switch-behavior-1] quit
```

Create QoS policy **1**, and associate traffic class **1** with traffic behavior **1** in the QoS policy.

```
[Switch] qos policy 1
[Switch-qospolicy-1] classifier 1 behavior 1
[Switch-qospolicy-1] quit
```

b. Verify that you can access VLANs 100 through 199. For example, apply QoS policy **1** to the incoming traffic of VLANs 100 through 107.

```
[Switch] qos vlan-policy 1 vlan 100 to 107 inbound
```

c. Verify that you cannot access any other VLANs except VLANs 100 through 199. For example, apply QoS policy **1** to the incoming traffic of VLANs 200 through 207.

```
[Switch] qos vlan-policy 1 vlan 200 to 207 inbound
Permission denied.
```

4. Verify that you can Telnet to the core switch by using the account **admin-departB@bbb** from Department B. (Details not shown.)

5. Verify that you have the access permission of user role **departB-resource**:

a. Verify that you can use all commands of the QoS and ACL features:

Create IPv4 advanced ACL 3001 and enter ACL view.

```
<Switch> system-view
[Switch] acl number 3001
```

Create an IPv4 advanced ACL rule to permit outbound FTP packets.

```
[Switch-acl-ipv4-adv-3001] rule permit tcp destination-port eq ftp-data
[Switch-acl-ipv4-adv-3001] quit
```

Create traffic class **2** and enter traffic class view.

```
[Switch] traffic classifier 2
```

Define a match criterion for traffic class **2** to match the advanced ACL 3001.

```
[Switch-classifier-2] if-match acl 3001
[Switch-classifier-2] quit
```

Create traffic behavior **2** and enter traffic behavior view.

```
[Switch] traffic behavior 2
```

Set the CIR of the CAR action to 2000 kbps.

```
[Switch-behavior-2] car cir 2000
[Switch-behavior-2] quit
```

Create QoS policy **2**, and associate traffic class **2** with traffic behavior **2** in the QoS policy.

```
[Switch] qos policy 2
[Switch-qospolicy-2] classifier 2 behavior 2
[Switch-qospolicy-2] quit
```

b. Verify that you can access VLANs 200 through 299. For example, apply QoS policy **2** to the incoming traffic of VLANs 200 through 207.

```
[Switch] qos vlan-policy 2 vlan 200 to 207 inbound
```

c. Verify that you cannot access any other VLANs except VLANs 200 through 299. For example, apply QoS policy **2** to the incoming traffic of VLANs 100 through 107.

```
[Switch] qos vlan-policy 2 vlan 100 to 107 inbound
Permission denied.
```

Configuration files

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface Vlan-interface3
 ip address 20.1.1.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/23
port access vlan 3
#
interface GigabitEthernet1/0/24
port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$JzDegvL0G5KZIcJhzscTHLA4WasBVh0UOw==
 key accounting cipher $c$3$CdejNYYxvjW0Y+Zydi4rZgBwjYb4h6LKmg==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
role name departA-resource
rule 1 permit read write execute feature qos
 rule 2 permit read write execute feature acl
 vlan policy deny
  permit vlan 100 to 199
 interface policy deny
 vpn-instance policy deny
#
role name departB-resource
rule 1 permit read write execute feature qos
 rule 2 permit read write execute feature acl
 vlan policy deny
  permit vlan 200 to 299
 interface policy deny
 vpn-instance policy deny
#
```

Contents

Introduction

This document provides software upgrade examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of FTP and TFTP.

General restrictions and guidelines

When you upgrade software, follow these restrictions and guidelines:

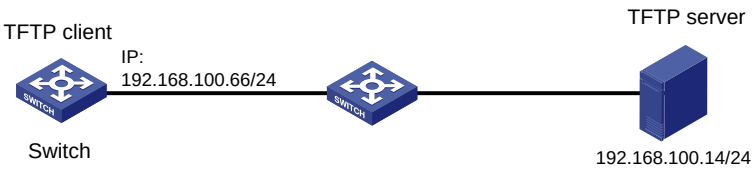
- Make sure the switch has sufficient storage space for the upgrade file. If the switch does not have sufficient storage space, delete unused files by using the **`delete /unreserved`** *`file-url`* command.
- Save the configuration before the upgrade for the configuration to survive a reboot.
- If the switch supports the management Ethernet interface, assign an IP address to the management Ethernet interface. If the switch does not support the management Ethernet interface, assign an IP address to VLAN-interface 1.

Example: Using the switch as a TFTP client to upgrade software

Network configuration

As shown in Figure 1, use TFTP to download a software upgrade file from a TFTP server to upgrade the switch.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

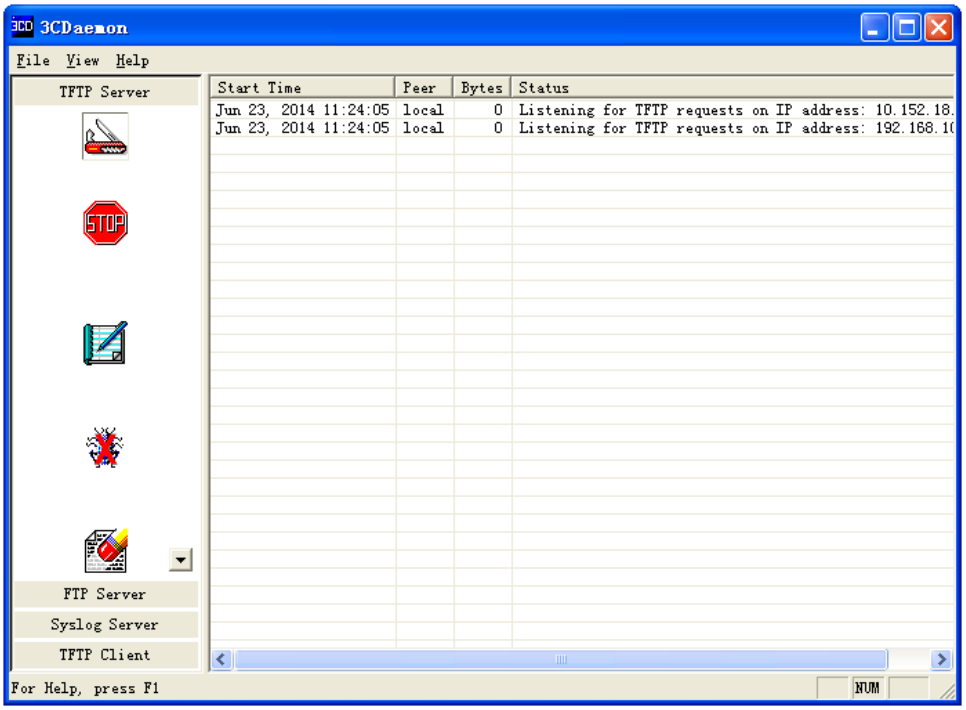
Procedures

1. Configure the TFTP server:

Assign the IP address 192.168.100.14/24 to the TFTP server. (Details not shown.)

Start the TFTP server and specify a working directory. This example uses the 3CDaemon TFTP server. (Details not shown.)

Figure 2 Configuring the TFTP server



2. Upgrade the switch:

(Switches supporting the management Ethernet interface) Assign an IP address to M-GigabitEthernet 0/0/0. Make sure the switch can reach the TFTP server.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface m-gigabitethernet 0/0/0
[Switch-M-GigabitEthernet0/0/0] ip address 192.168.100.66 255.255.255.0
[Switch-M-GigabitEthernet0/0/0] quit
[Switch] quit
```

(Switches not supporting the management Ethernet interface) Assign an IP address to VLAN-interface 1. Make sure the switch can reach the TFTP server.

```
<Switch> system-view
[Switch] interface Vlan-interface1
[Switch-Vlan-interface1] ip address 192.168.100.66 255.255.255.0
[Switch-Vlan-interface1] quit
```

Verify that the switch can ping the TFTP server.

```
<Switch> ping 192.168.100.14
Ping 192.168.100.14 (192.168.100.14): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.100.14: icmp_seq=0 ttl=64 time=10.701 ms
56 bytes from 192.168.100.14: icmp_seq=1 ttl=64 time=2.678 ms
56 bytes from 192.168.100.14: icmp_seq=2 ttl=64 time=2.282 ms
56 bytes from 192.168.100.14: icmp_seq=3 ttl=64 time=1.617 ms
56 bytes from 192.168.100.14: icmp_seq=4 ttl=64 time=1.701 ms

--- Ping statistics for 192.168.100.14 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.617/3.796/10.701/3.474 ms
```

Save the configuration.

```
<Switch> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Use TFTP to download the upgrade file **switch.ipe** from the TFTP server to the root directory of the storage medium on the switch.

```
<Switch> tftp 192.168.100.14 get switch.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 58.7M  100 58.7M    0     0  1193k      0  0:00:50  0:00:50 --:--:-- 1127k
```

Specify **switch.ipe** as the main startup image file.

```
<Switch> boot-loader file flash:/switch.ipe slot 1 main
Verifying the file flash:/switch.ipe on slot 1.....Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file switch.bin to flash:/boot.bin.........Done.
Decompressing file switch.bin to flash:/system.bin.........................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Reboot the switch.

```
<Switch> reboot
```

Verifying the configuration

Verify that the software has been upgraded.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5130S-52S-HI uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot

Boot image: flash:/boot.bin
Boot image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
System image: flash:/system.bin
System image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
---- More ----
```

Display the current software images and startup software images.

```
<Switch> display boot-loader
Software images on slot 1:
```

```
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
None
```

Configuration files

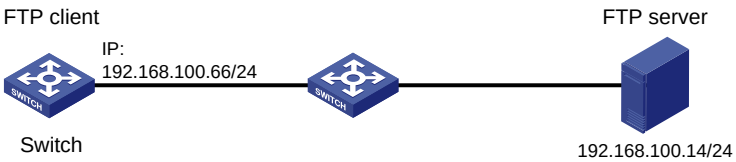
- Switches supporting the management Ethernet interface:
  ```
  #
  interface M-GigabitEthernet0/0/0
  ip address 192.168.100.66 255.255.255.0
  #
  ```
- Switches not supporting the management Ethernet interface:
  ```
  #
  interface Vlan-interface1
  ip address 192.168.100.66 255.255.255.0
  #
  ```

Example: Using the switch as an FTP client to upgrade software

Network configuration

As shown in Figure 3, use FTP to download a software upgrade file from an FTP server to upgrade the switch.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

1. Configure the FTP server:

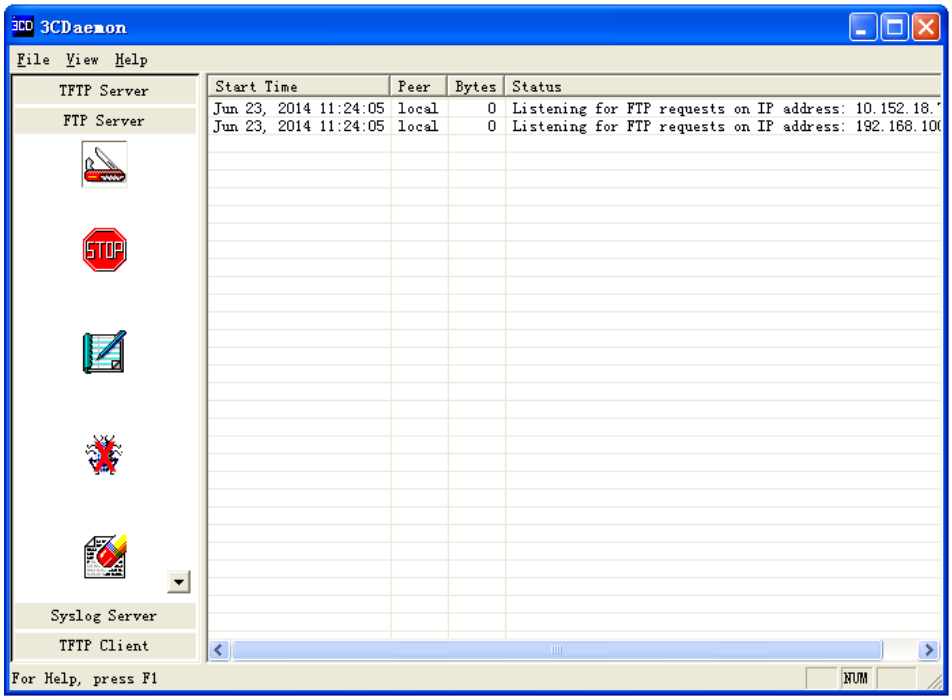
Assign the IP address 192.168.100.14/24 to the FTP server. (Details not shown.)

Start the FTP server and specify a working directory. This example uses the 3CDaemon FTP server. (Details not shown.)

Add a local user account. (Details not shown.)

Set the username to **123456** and the password to **123456** for the user account.

Figure 4 Configuring the FTP server



2. Upgrade the switch:

(Switches supporting the management Ethernet interface) Assign an IP address to M-GigabitEthernet 0/0/0. Make sure the switch can reach the FTP server.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface m-gigabitethernet 0/0/0
[Switch-M-GigabitEthernet0/0/0] ip address 192.168.100.66 255.255.255.0
[Switch-M-GigabitEthernet0/0/0] quit
[Switch] quit
```

(Switches not supporting the management Ethernet interface) Assign an IP address to VLAN-interface 1. Make sure the switch can reach the TFTP server.

```
<Switch> system-view
[Switch] interface Vlan-interface1
[Switch-Vlan-interface1] ip address 192.168.100.66 255.255.255.0
[Switch-Vlan-interface1] quit
```

Verify that the switch can ping the FTP server.

```
<Switch> ping 192.168.100.14
Ping 192.168.100.14 (192.168.100.14): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.100.14: icmp_seq=0 ttl=64 time=10.701 ms
56 bytes from 192.168.100.14: icmp_seq=1 ttl=64 time=2.678 ms
56 bytes from 192.168.100.14: icmp_seq=2 ttl=64 time=2.282 ms
56 bytes from 192.168.100.14: icmp_seq=3 ttl=64 time=1.617 ms
56 bytes from 192.168.100.14: icmp_seq=4 ttl=64 time=1.701 ms

--- Ping statistics for 192.168.100.14 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.617/3.796/10.701/3.474 ms
```

Save the configuration.

```
<Switch> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to  mainboard device successfully.
```

Use the username **123456** and the password **123456** to log in to the FTP server.

```
<Switch> ftp 192.168.100.14
Connected to 192.168.100.14 (192.168.100.14).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.100.14:(none)): 123456
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
```

Use FTP to download the upgrade file **switch.ipe** from the FTP server to the root directory of the storage medium on the switch.

```
ftp> get switch.ipe
227 Entering passive mode (192,168,100,14,8,86)
125 Using existing data connection
226 Closing data connection; File transfer successful.
50445056 bytes received in 53.6 seconds (1.25 Mbyte/s)
ftp> quit
```

Specify **switch.ipe** as the main startup image file.

```
<Switch> boot-loader file flash:/switch.ipe slot 1 main
Verifying the file flash:/switch.ipe on slot 1.....Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file switch.bin to flash:/boot.bin.........Done.
Decompressing file switch.bin to
flash:/system.bin.............................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on on slot 1.
```

Reboot the switch.

```
<Switch> reboot
```

Verifying the configuration

Verify that the software has been upgraded.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
```

```
H3C S5130S-52S-HI uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot

Boot image: flash:/boot.bin
Boot image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
System image: flash:/system.bin
System image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
---- More ----
```

Display the current software images and startup software images.

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
None
```

Configuration files

- Switches supporting the management Ethernet interface:
  ```
  #
  interface M-GigabitEthernet0/0/0
  ip address 192.168.100.66 255.255.255.0
  #
  ```
- Switches not supporting the management Ethernet interface:
  ```
  #
  interface Vlan-interface1
  ip address 192.168.100.66 255.255.255.0
  #
  ```

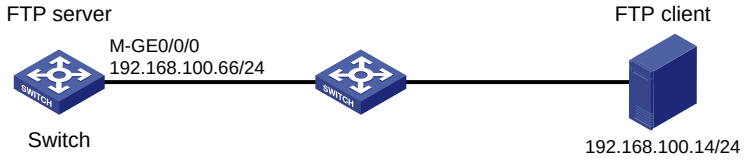
Example: Using the switch as an FTP server to upgrade software

Network configuration

As shown in Figure 5:

- Enable the FTP server on the switch.
- Use FTP to upload a software upgrade file from an FTP client to upgrade the switch.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Analysis

To use the switch as an FTP server, you must create a local user account on the switch to provide FTP service.

Restrictions and guidelines

You must set the file transfer mode to binary for FTP to transfer files correctly.

Procedures

1. Configure the FTP server:

(Switches supporting the management Ethernet interface) Assign an IP address to M-GigabitEthernet 0/0/0.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] interface m-gigabitethernet 0/0/0
[Switch-M-GigabitEthernet0/0/0] ip address 192.168.100.66 255.255.255.0
[Switch-M-GigabitEthernet0/0/0] quit
```

(Switches not supporting the management Ethernet interface) Assign an IP address to VLAN-interface 1. Make sure the switch can reach the TFTP server.

```
<Switch> system-view
[Switch] interface Vlan-interface1
[Switch-Vlan-interface1] ip address 192.168.100.66 255.255.255.0
[Switch-Vlan-interface1] quit
```

Add a local user account. Set the username to **abc** and the password to **a123456789**.

```
[Switch] local-user abc
[Switch-luser-abc] password simple a123456789
```

Assign the network-admin user role to the user account.

```
[Switch-luser-abc] authorization-attribute user-role network-admin
```

Remove the default network-operator user role.

```
[Switch-luser-abc] undo authorization-attribute user-role network-operator
```

Assign FTP service to the user account.

```
[Switch-luser-abc] service-type ftp
[Switch-luser-abc] quit
# Enable the FTP server.
[Switch] ftp server enable
[Switch] quit
```

Save the configuration.

```
<Switch> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
```

```
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

2. Configure the FTP client:

Assign the IP address 192.168.100.14/24 to the FTP client. Make sure the FTP client can reach the switch. (Details not shown.)

Use the username **abc** and the password **a123456789** to log in to the FTP server.

```
C:\Documents and Settings\Administrator> ftp 192.168.100.66
Connected to 192.168.100.66.
220 FTP service ready.
User (192.168.100.66:(none)): abc
331 Password required for abc.
Password:
230 User logged in.
```

Access the directory that contains the upgrade file.

```
ftp> lcd E:\
Local directory now E:\
```

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Transfer the upgrade file **switch.ipe** to the root directory of the storage medium on the FTP server.

```
ftp> put switch.ipe
200 PORT command successful
150 Connecting to port 2903
226 File successfully transferred
ftp: 50445056 sent in 1.05Seconds 67282.77Kbytes/sec.
```

Verify that the image file is saved on the FTP server.

```
ftp> ls switch.ipe
200 PORT command successful
150 Connecting to port 3391
switch.ipe
226 1 matches total
ftp: 24 bytes received in 0.00Seconds 24000.00Kbytes/sec.
```

Close the FTP connection.

```
ftp> bye
```

3. Upgrade the switch:

Specify **switch.ipe** as the main startup image file.

```
<Switch> boot-loader file flash:/switch.ipe slot 1 main
Verifying the IPE file and the images.....Done.
Verifying the file flash:/switch.ipe on slot 1.....Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
```

```
Decompressing file switch.bin to flash:/boot.bin.........Done.
Decompressing file switch.bin to
flash:/system.bin................................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Reboot the switch.

```
<Switch> reboot
```

Verifying the configuration

Verify that the software has been upgraded.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5130S-52S-HI uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot

Boot image: flash:/boot.bin
Boot image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
System image: flash:/system.bin
System image version: 7.1.070, Release xxxx
  Compiled Jun 18 2019 17:52:09
---- More ----
```

Display the current software images and startup software images.

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
None
```

Configuration files

- Switches supporting the management Ethernet interface:

```
#
interface M-GigabitEthernet0/0/0
ip address 192.168.100.66 255.255.255.0
#
local-user abc class manage
 password hash
$h$6$YMVbbwFL/vviWcQu$+CuTbYCehNZtZo5RCXiadpYbXYWa2omt5TUtEh3UPCg3fZjxYCp5WzbuE2G
oowVi2YA/BK+mnSZJZqi5jRDuCg==
 service-type ftp
```

```
 authorization-attribute user-role network-admin
#
 ftp server enable
#
```

- Switches not supporting the management Ethernet interface:

```
#
interface Vlan-interface1
ip address 192.168.100.66 255.255.255.0
#
local-user abc class manage
 password hash
$h$6$YMVbbwFL/vviWcQu$+CuTbYCehNZtZo5RCXiadpYbXYWa2omt5TUtEh3UPCg3fZjxYCp5WzbuE2G
oowVi2YA/BK+mnSZJZqi5jRDuCg==
 service-type ftp
 authorization-attribute user-role network-admin
#
 ftp server enable
#
```

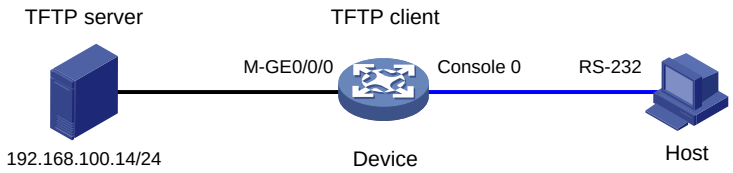
Example: Using the device as a TFTP client to upgrade software

Network configuration

As shown in Figure 6, the device cannot start up.

Use TFTP to upgrade the device from the BootWare menu.

Figure 6 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you upgrade software, make sure the device has sufficient storage space for the upgrade file. If the device does not have sufficient storage space, delete unused files by using the **delete /unreserved** *file-url* command.

Procedures

1. Configure the host:

   # Use a console cable to connect console port 0 on the device to the configuration terminal. (Details not shown.)

To access the device through the console port, you must run a terminal emulator program (HyperTerminal, PuTTY, or Tera Term) on the host. For information about using a terminal emulator program, see the program's user guide.

The following are the required terminal settings:

- **Baud rate**—9600.
- **Data bits**—8.
- **Stop bits**—1.
- **Parity**—none.
- **Flow control**—none.

2. Configure the TFTP server:

Assign the IP address 192.168.100.14/24 to the TFTP server. (Details not shown.)

Start the TFTP server and specify a working directory.

3. Upgrade the device:

The BootWare menu varies by device model. This section uses S6550XE-56HF-HI as an example.

Use a straight-through Ethernet cable to connect the management Ethernet interface (M-GigabitEthernet 0/0/0) on the device to the TFTP server.

Save the running configuration.

```
<Device> system-view
[Device] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
[Device] quit
```

Reboot the device.

```
<Device> reboot
```

Press **Ctrl**+**B** at prompt to access the EXTEND-BOOTWARE menu.

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU...
Press Ctrl+T to start heavy memory test
Booting extended BootRom
The extended BootRom is self-decompressing......Done.

********************************************************************************
*                                                                              *
*                H3C S6550XE-56HF-HI BOOTROM, Version 103                      *
*                                                                              *
********************************************************************************
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.

Creation Date       : Mar 30 2021
Memory Type         : DDR4 SDRAM
Memory Size         : 3072MB
Memory Speed        : 800MHz
Flash Size          : 1024MB
```

```
CPLD 1 Version       : 001
CPLD 2 Version       : 001
CPLD 3 Version       : 001
PCB 1 Version        : Ver.A
PCB 2 Version        : Ver.B
Mac Address         : 346b5bebf2ed


Press Ctrl+B to access EXTENDED BOOT MENU...0

Password recovery capability is enabled.

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
9. Set The Operating Device
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Enter your choice(0-9):
```

Press **1** to access the file transfer protocol menu.

```
Enter your choice(0-9): 1
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

Press **1** to configure the network parameters.

```
Enter your choice(0-3): 1
Load File Name    : s6550xe-h3c-test.ipe
                :
Server IP Address  :192.168.0.30
Local IP Address   :192.168.0.20
Subnet Mask       :0.0.0.0
Gateway IP Address :0.0.0.0

Loading... Done.
```

Table 1 Network parameter fields

Field	Description
Load File Name	Set the name of the file to be downloaded.
Server IP Address	Set the IP address of the TFTP server.
Local IP Address	Set the IP address of the interface that connects to the TFTP server.
Subnet Mask	Set the IP address mask.
Target File Name	Set a file name for saving the file on the device. By default, the target file name is the same as the source file name.
Gateway IP Address	Set a gateway IP address if the router is on a different network from the server.

Press **Enter** and enter **Y** at prompt to download the file.

```
Are you sure to download file to flash? Yes or No (Y/N):Y
Loading.....................................................................
.....................................................................
.....................................................................
.....................................................Done.
```

Assign image file attribute main (M) to the file. The EXTEND-BOOTWARE menu appears again.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash.....................................................................
.....................................................................
.....................................................Done.
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................Done.

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
9. Set The Operating Device
```

```
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright

Enter your choice(0-9):
```

Enter **0** in the EXTEND-BOOTWARE menu to reboot the device.

```
Enter your choice(0-9): 0
Loading the main image files...
Loading file flash:/s6550xe-cmw710-system-test.bin.....................
.....................................................................
.....................................................................
.....................Done.
Loading file flash:/s6550xe-cmw710-boot-test.bin.....................
....Done.

Image file flash:/s6550xe-cmw710-boot-test.bin is self-decompressing......
................................................Done.
System image is starting...
Line aux1 is available.


Press ENTER to get started.
```

Verifying the configuration

1. Verify that the software has been upgraded.

```
<Device> display version
H3C Comware Software, Version 7.1.070, Release 8106P22
Copyright (c) 2004-2022 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S6550XE-56HF-HI uptime is 0 weeks, 0 days, 5 hours, 45 minutes
Last reboot reason : User reboot

Boot image: flash:/s6550xe-cmw710-boot-test.bin
Boot image version: 7.1.070, Release 8106P22
  Compiled Nov 19 2022 11:00:00
System image: flash:/s6550xe-cmw710-system-test.bin
System image version: 7.1.070, Release 8106P22
  Compiled Nov 19 2022 11:00:00
---- More ----
```

2. Verify that the startup software images are as configured.

```
<Device> display boot-loader slot 1
Software images on slot 1:
Current software images:
  flash:/s6550xe-cmw710-boot-test.bin
  flash:/s6550xe-cmw710-system-test.bin
```

```
Main startup software images:
  flash:/s6550xe-cmw710-boot-test.bin
  flash:/s6550xe-cmw710-system-test.bin
Backup startup software images:
  flash:/s6550xe-cmw710-boot-old.bin
  flash:/s6550xe-cmw710-system- old.bin
```

Configuration files

The system does not save the commands used in this procedure to a configuration file.

Contents

Introduction

This document provides compatible and incompatible ISSU configuration examples.

Before performing an ISSU, use the **display version comp-matrix file** command to view the recommended ISSU method in the **Upgrade Way** field. Table 1 shows a matrix of ISSU types and ISSU methods.

Table 1 Matrix of ISSU types and ISSU methods

ISSU type	ISSU methods
Compatible	The ISSU methods are displayed in the **Upgrade Way** field. • Service Upgrade • File Upgrade • ISSU Reboot • Reboot
Incompatible	Only one upgrade method (**Incompatible upgrade**) is available, which is displayed at the end of command output.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of ISSU.

General restrictions and guidelines

Before performing an ISSU, you must complete the following preparation tasks:

- Read the software release notes to identify support of the device for ISSU.
- Use the **display device** command to verify that no member devices are in **Fault** state.
- Use the **dir** command to verify that the device has sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files.
- For service continuity during an ISSU, verify that the following feature settings are configured:

Feature	Setting requirements
GR/NSR	Enable GR or NSR for protocols including LDP, RSVP, OSPF, ISIS, BGP, and FSPF.
BFD	Disable BFD for protocols including LDP, RSVP, OSPF, ISIS, RIP, BGP, VRRP, and NQA.
Ethernet link aggregation	Use the long LACP timeout interval (the **lacp period short** command is not configured) on all member ports in dynamic aggregation groups.
IRF	Configure IRF bridge MAC persistence as follows: • **Compatible upgrade**—Configure the **irf mac-address persistent timer** or **irf mac-address persistent always** command. • **Incompatible upgrade** ○ Configure the **irf mac-address persistent always**

Feature	Setting requirements
	command if the bridge MAC address is the MAC address of the device for which you want to execute the **issu load** command. ○ Disable IRF MAD before the ISSU and enable IRF MAD again after the ISSU.

- Log in to the device through the console port. If you use Telnet or SSH, you might be disconnected from the device before the ISSU is completed.

During an ISSU, use the following guidelines:

- In a multiuser environment, make sure no other administrators access the device while you are performing the ISSU.
- Do not perform any of the following tasks during an ISSU:
  - Reboot, add, or remove member device.
  - Execute commands that are not for ISSU.
  - Modify, delete, or rename image files.

The following describes restrictions and guidelines for an ISSU.

Hardware requirements

- Log in to the device through the console port. If you use Telnet or SSH, you might be disconnected from the device before the ISSU is completed.
- Do not perform an ISSU during hardware upgrade or failure. Otherwise, upgrade failure or system exceptions might occur.

Upgrade restrictions

- Use the **display device** command to verify that no member devices are in **Fault** state.
- Use the **dir** command to verify that the device has sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files by using the **delete** command.

Feature restrictions

For service continuity during ISSU, configure the following feature settings:

Feature	Setting requirements
GR or NSR	Enable GR or NSR for protocols including LDP, RSVP, OSPF, ISIS, BGP, and FSPF.
BFD	Disable BFD for protocols including LDP, RSVP, OSPF, ISIS, RIP, BGP, VRRP, and NQA.
Ethernet link aggregation	Use the long LACP timeout interval (the **lacp period short** command is not configured) on all member ports in dynamic aggregation groups.
IRF	Configure IRF bridge MAC persistence as follows: • **Compatible upgrade**—Configure the **irf mac-address persistent timer** or **irf mac-address persistent always** command. • **Incompatible upgrade**—Configure the **irf mac-address persistent always** command if the bridge MAC address is the MAC address of the device for which you want to execute the **issu load** command.

Operation restrictions

- In a multiuser environment, make sure no other administrators access the device while you are performing the ISSU.

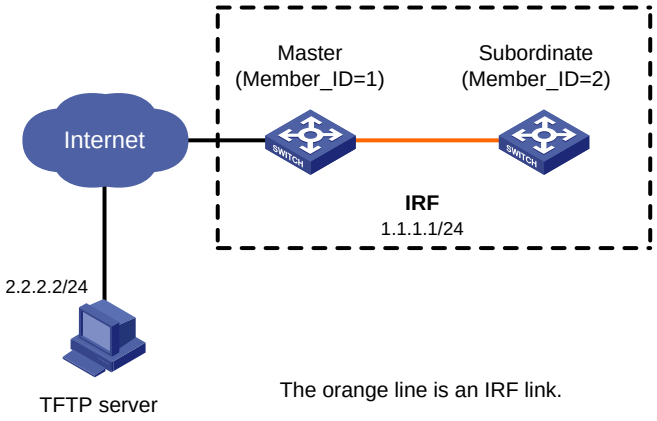
- Do not perform any of the following tasks during an ISSU:
  - Reboot, add, or remove member device.
  - Execute commands that are irrelevant to the ISSU.
  - Modify, delete, or rename image files.

Example: Performing a compatible ISSU

Network configuration

As shown in Figure 1, the two-chassis IRF fabric and the TFTP server can reach each other. Perform a compatible ISSU on the IRF to upgrade startup images from T0001015 to T0001016.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported

S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you perform the compatible ISSU, follow these restrictions and guidelines:

- The available storage space on each member device must be at least two times the size of the new image.
- Do not execute commands that are irrelevant to the ISSU.
- The automatic rollback timer starts after you execute the **issu run switchover** command. If no exceptions occur, execute the **issu accept** or **issu commit** command to complete the upgrade before this timer expires. If an exception occurs, manually roll back or wait for the system to automatically roll back to the original software images, and then perform a new upgrade.
- After you execute the **issu accept** or **issu commit** command, the system automatically deletes the rollback timer.

Procedures

Download the new image file T0001016.ipe from the TFTP server to the root directory of a file system on the master. The .ipe file includes the boot-t0001016.bin image file and the system-t0001016.bin image file.

```
<Sysname> tftp 2.2.2.2 get T0001016.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 52.2M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165
```

Display current software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
```

Display the recommended ISSU methods.

```
<Sysname> display version comp-matrix file ipe flash:/T0001016.ipe
Verifying the file flash:/T0001016.ipe on slot 1.................................Done.
Identifying the upgrade methods...........Done.

  Slot                          Upgrade Way
  1                             Reboot
  2                             Reboot
```

The output shows the two versions are compatible and a reboot is needed to complete upgrade.

Set the rollback timer to 120 minutes (the default is 45 minutes).

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] issu rollback-timer 120
<Sysname> quit
```

Upgrade the subordinate member.

```
<Sysname> issu load file ipe flash:/T0001016.ipe slot 2
This operation will delete the rollback point information for the previous upgrade
 and maybe get unsaved configuration lost. Continue? [Y/N]:y
Successfully copied flash:/boot-t0001016.bin to slot2#flash:/boot-t0001016.bin.
Successfully copied flash:/system-t0001016.bin to slot2#flash:/system-t0001016.bin.
Upgrade summary according to following table:

flash:/boot-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/system-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                          Upgrade Way
  2                             Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

After the subordinate member starts up, verify that the ISSU is finished on the subordinate member.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Incompatible
Work state: Normal
```

```
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 2
Previous version list:
  boot: 7.1.070 Test 0001015
  system: 7.1.070 Test 0001015
Upgrade version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
```

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/boot-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/system-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Switchover Way
  1                           Master subordinate switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

Verify that the switchover has completed.

```
<Sysname> display issu state
ISSU state: switchover
Compatibility: Unknown
Work state: Normal
Upgrade method: card by card
Upgraded chassis: None
Current upgrading chassis: None
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
```

// The ISSU state Switchover indicates the switchover has completed.

Upgrade the original master.

```
<Sysname> issu commit slot 1
Upgrade summary according to following table:

flash: /boot-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016
```

```
flash: /system-t0001016.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

View ISSU state.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: card by card
Upgraded chassis: None
Current upgrading chassis: None
Current version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
Current software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
```

// The Init state indicates that the ISSU has completed.

Verifying the configuration

Verify that startup images have been upgraded to T0001016.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
Active packages on slot 2:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
```

Configuration files

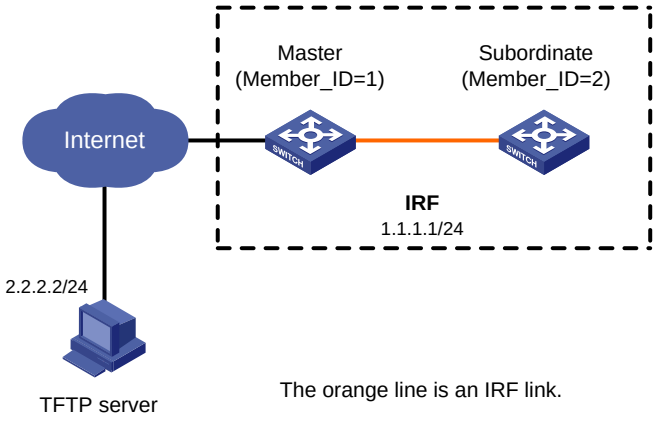
The system does not save the commands used in the configuration procedures to a configuration file.

Example: Performing an incompatible ISSU

Network configuration

As shown in Figure 2, the two-chassis IRF fabric and the TFTP server can reach each other. Perform an incompatible ISSU on the IRF to upgrade startup images from T0001015 to T0001017.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-28S MS4520V2-24TP	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported

E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you perform the incompatible ISSU, follow these restrictions and guidelines:

- The available storage space on each member device must be at least two times the size of the new image.
- Do not execute commands that are irrelevant to the ISSU.

Procedures

Download the new image file T0001017.ipe from the TFTP server to the root directory of a file system on the master. The .ipe file includes the boot-t0001017.bin image file and the system-t0001017.bin image file.

```
<Sysname> tftp 2.2.2.2 get T0001017.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 50.1M  100 42.8M    0     0   159k      0  0:04:34  0:04:34 --:--:--  165k
```

Display current software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
```

Display the ISSU method.

```
<Sysname> display version comp-matrix file ipe flash:/T0001017.ipe
Verifying the file flash:/T0001017.ipe on slot 1.................................Done.
Identifying the upgrade methods...........Done.
Incompatible upgrade.
```

The output shows the two versions are incompatible and a reboot is needed to complete upgrade.

Upgrade the subordinate member.

```
<Sysname> issu load file ipe flash:/T0001017.ipe slot 2
This operation will delete the rollback point information for the previous upgrade
and maybe get unsaved configuration lost. Continue? [Y/N]:y
Successfully copied flash:/boot-t0001017.bin to slot2#flash:/boot-t0001017.bin.
Successfully copied flash:/system-t0001017.bin to slot2#flash:/system-t0001017.bin.

flash:/boot-t0001017.bin
  Running Version             New Version
  Test 0001015                Test 0001017

flash:/system-t0001017.bin
  Running Version             New Version
  Test 0001015                Test 0001017

  Slot                        Upgrade Way
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]: y
```

Verify that the ISSU is finished on the subordinate member.

```
<Sysname> display issu state
ISSU state: Loaded
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 2
Previous version list:
  boot: 7.1.070 Test 0001015
  system: 7.1.070 Test 0001015
Upgrade version list:
  boot: 7.1.070, Test 0001017
  system: 7.1.070, Test 0001017
```

Perform a master/subordinate switchover to complete upgrade.

```
<Sysname> issu run switchover
Successfully copied flash:/boot-t0001017.bin to slot2#flash:/boot-t0001017.bin.
Successfully copied flash:/system-t0001017.bin to slot2#flash:/system-t0001017.bin.

flash:/boot-t0001017.bin
  Running Version             New Version
  Test 0001015                Test 0001017
```

```
flash:/system-t0001017.bin
  Running Version             New Version
  Test 0001015                Test 0001017

  Slot                        Upgrade Way
  2                           Reboot
  1                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
```

View ISSU state.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: card by card
Upgraded chassis: None
Current upgrading chassis: None
Current version list:
  boot: 7.1.070, Test 0001017
  system: 7.1.070, Test 0001017
Current software images:
  flash:/boot-t0001017.bin
  flash:/system-t0001017.bin
```

// The Init state indicates that the ISSU has completed.

Verifying the configuration

Verify that startup images have been upgraded to T0001017.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001017.bin
  flash:/system-t0001017.bin
Active packages on slot 2:
  flash:/boot-t0001017.bin
  flash:/system-t0001017.bin
```

Configuration files

The system does not save the commands used in the configuration procedures to a configuration file.

Contents

Introduction

This document provides software patching examples that use **`install`** commands.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

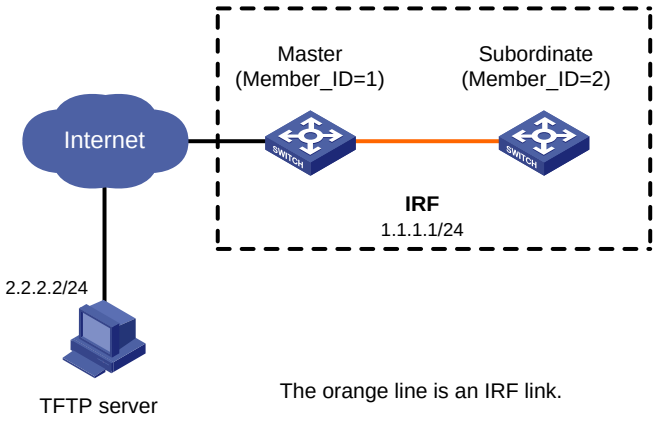
Example: Patching software

Network configuration

As shown in Figure 1, the two-chassis IRF fabric and the TFTP server can reach each other. The IRF members are running CMW710-SYSTEM-R6312, and they have not been patched before.

Use the patch image file CMW710-SYSTEM-R6312H04.bin to fix bugs without rebooting the members.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx

S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx

S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you patch software for a centralized IRF device, follow these restrictions and guidelines:

- The first time you install patch images, you must start with the master. For subsequent patch installations, you must start with the subordinate members.
- The patch image version must match the device model and Comware version. For example, to fix bugs in CMW710-SYSTEM-R6312.bin, you must use CMW710-SYSTEM-R6312H04.bin.

Procedures

Download the patch image file CMW710-SYSTEM-R6312H04.bin from the TFTP server to the root directory of the flash memory on the master.

```
<Sysname> tftp 2.2.2.2 get CMW710-SYSTEM-R6312H04.bin
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
```

```
                                 Dload  Upload   Total   Spent    Left  Speed
100 25.2M    0 25.2M    0     0   210k      0 --:--:--  0:02:02 --:--:--  209k
```

Activate the patch images on the master first and then on the subordinate member. This sequence is used because no patch images have been activated on the IRF fabric.

```
<Sysname> install activate patch flash:/CMW710-SYSTEM-R6312H04.bin slot 1
This operation maybe take several minutes, please wait.............Done.
<Sysname> install activate patch flash:/CMW710-SYSTEM-R6312H04.bin slot 2
This operation maybe take several minutes, please wait.............Done.
```

The patch images take effect immediately after they are activated.

For the patch images to take effect after a reboot, commit the software changes.

```
<Sysname> install commit
```

Verifying the configuration

Verify that the patch images have been activated successfully.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/CMW710-BOOT-R6312.bin
  flash:/CMW710-SYSTEM-R6312.bin
  flash:/CMW710-SYSTEM-R6312H04.bin
Active packages on slot 2:
  flash:/CMW710-BOOT-R6312.bin
  flash:/CMW710-SYSTEM-R6312.bin
  flash:/CMW710-SYSTEM-R6312H04.bin
```

Verify that the patch image file has been added to the main startup software image list so the images can take effect after a reboot.

```
<Sysname> display install committed
Committed packages on slot 1:
  flash:/CMW710-BOOT-R6312.bin
  flash:/CMW710-SYSTEM-R6312.bin
  flash:/CMW710-SYSTEM-R6312H04.bin
Committed packages on slot 2:
  flash:/CMW710-BOOT-R6312.bin
  flash:/CMW710-SYSTEM-R6312.bin
  flash:/CMW710-SYSTEM-R6312H04.bin
```

Configuration files

The system does not save the commands used in the configuration procedures to a configuration file.

Contents

Introduction

This document provides Ethernet link aggregation configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of Ethernet link aggregation.

Example: Configuring Layer 2 link aggregation

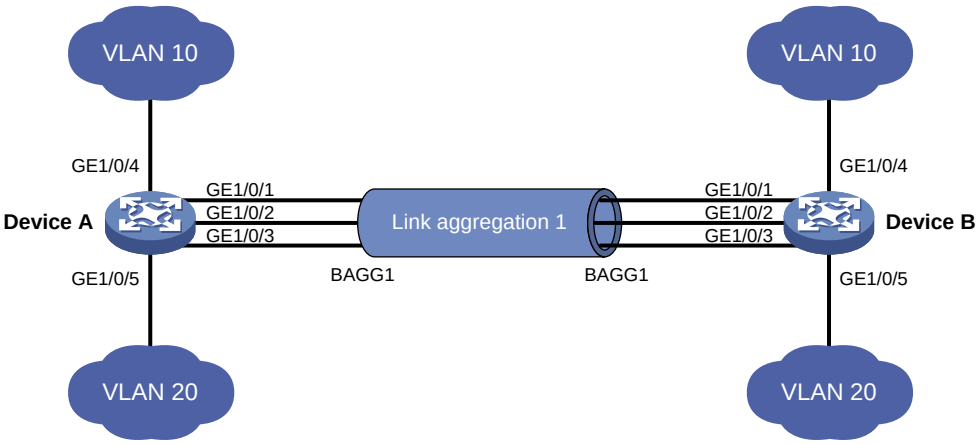
Network configuration

As shown in Figure 1, both Device A and Device B forward traffic from VLAN 10 and VLAN 20.

Configure link aggregation on Device A and Device B to meet the following requirements:

- VLAN 10 on Device A can communicate with VLAN 10 on Device B.
- VLAN 20 on Device A can communicate with VLAN 20 on Device B.

Figure 1 Network diagram



Analysis

To enable traffic from VLAN 10 and VLAN 20 to pass through Layer 2 aggregate interface Bridge-aggregation 1, perform the following tasks:

- Configure Layer 2 aggregate interface Bridge-aggregation 1 as a trunk port.
- Assign the aggregate interface to VLAN 10 and VLAN 20.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure Layer 2 link aggregation, follow these restrictions and guidelines:

- When you assign a port to an aggregation group, the recommended configuration procedure is as follows:
  a. Use the **display this** command in interface view to check the following attribute configurations of the port:
    - Port isolation.
    - QinQ.
    - VLAN.
    - VLAN mapping.

  b. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.

  c. Assign the port to the aggregation group.
- In a static aggregation group, the Selected state of a port is not affected by whether the peer port is added to an aggregation group and is Selected. As a result, the Selected state of a port might be different from the Selected state of the peer port. When both ends support static aggregation and dynamic aggregation, use dynamic aggregation.
- You cannot assign a port to a Layer 2 aggregation group when MAC authentication, port security mode, or 802.1X is configured or enabled on the port.

Procedures

1. Configure Device A:

Create VLAN 10, and assign port GigabitEthernet 1/0/4 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

Create VLAN 20, and assign port GigabitEthernet 1/0/5 to VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

Create Layer 2 aggregate interface Bridge-aggregation 1. Use one of the following methods as needed.

- Use the static aggregation mode to create Layer 2 aggregate interface Bridge-aggregation 1.

  ```
  [DeviceA] interface bridge-aggregation 1
  [DeviceA-Bridge-Aggregation1] quit
  ```

- Use the dynamic aggregation mode to create Layer 2 aggregate interface Bridge-aggregation 1.

  ```
  [DeviceA] interface bridge-aggregation 1
  [DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
  [DeviceA-Bridge-Aggregation1] quit
  ```

Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

```
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

Configure Layer 2 aggregate interface Bridge-aggregation 1 as a trunk port.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
 Configuring GigabitEthernet1/0/1 done.
 Configuring GigabitEthernet1/0/2 done.
 Configuring GigabitEthernet1/0/3 done.
```

Assign the aggregate interface to VLANs 10 and 20.

```
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
 Configuring GigabitEthernet1/0/1 done.
 Configuring GigabitEthernet1/0/2 done.
 Configuring GigabitEthernet1/0/3 done.
[DeviceA-Bridge-Aggregation1] quit
```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about the link aggregation groups on Device A.

- Link aggregation configuration information when the static aggregation mode is used:

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port            Status  Priority  Oper-Key
  GE1/0/1(R)      S       32768     1
  GE1/0/2         S       32768     1
  GE1/0/3         S       32768     1
```

  The output shows that all member ports in the local aggregation group are in the Selected state. The Selected states of the local member ports are not affected by the Selected states of the peer member ports.

- Link aggregation configuration information when the dynamic aggregation mode is used:

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

```
Aggregation Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e234-5678
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    2        1                      {ACDEF}
  GE1/0/2             S        32768    3        1                      {ACDEF}
  GE1/0/3             S        32768    4        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    2        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/2             32768    3        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/3             32768    4        1        0x8000, a4e5-c316-0100 {ACDEF}
```

The output shows that the local member ports and the corresponding peer member ports are all Selected. In the dynamic link aggregation mode, each local member port and its peer member port have the same Selected state through exchanging LACPDUs. The user data traffic can be forwarded correctly.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 20
```

  - In the static aggregation mode:

```
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 10 20
```

  - In the dynamic aggregation mode:

```
#
interface Bridge-Aggregation1
port link-type trunk
```

```
port trunk permit vlan 10 20
link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-mode bridge
port link-type trunk
port trunk permit vlan 10 20
port link-aggregation group 1
#
```

- Device B:
  The configuration file on Device B is the same as the configuration file on Device A.

Example: Configuring Layer 2 aggregation load sharing

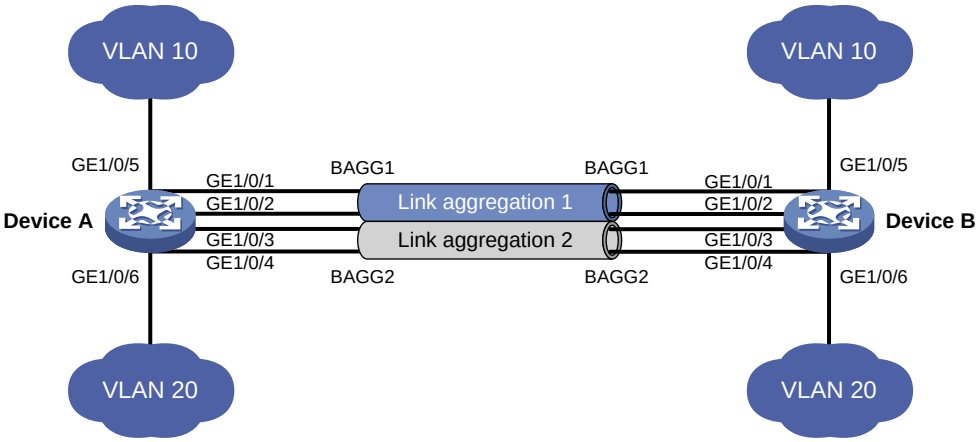
Network configuration

As shown in Figure 2, both Device A and Device B forward traffic for VLAN 10 and VLAN 20.

Configure link aggregation on Device A and Device B to meet the following requirements:

- Configure Layer 2 static aggregation groups 1 and 2 on both Device A and Device B.
- Configure link aggregation group 1 to forward traffic for VLAN 10.
- Configure link aggregation group 2 to forward traffic for VLAN 20.
- Configure link aggregation groups 1 and 2 to load share traffic across aggregation group member ports.
  - Configure link aggregation group 1 to load share packets based on source MAC addresses.
  - Configure link aggregation group 2 to load share packets based on destination MAC addresses.

Figure 2 Network diagram



Analysis

To enable the aggregate interfaces to forward traffic for VLAN 10 and VLAN 20, perform the following tasks:

- Assign Layer 2 aggregate interface Bridge-aggregation 1 to VLAN 10.
- Assign Layer 2 aggregate interface Bridge-aggregation 2 to VLAN 20.

For Bridge-aggregation 1 and Bridge-aggregation 2 to load share traffic across their Selected ports, set the load sharing mode in aggregate interface view.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported

S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported

MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you assign a port to an aggregation group, the recommended configuration procedure is as follows:

1. Use the **`display this`** command in interface view to check the following attribute configurations of the port:
   - Port isolation.
   - QinQ.
   - VLAN.
   - VLAN mapping.
2. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.
3. Assign the port to the aggregation group.

You cannot assign a port to a Layer 2 aggregation group when MAC authentication, port security mode, or 802.1X is configured or enabled on the port.

Procedures

Configuring Device A

Create VLAN 10, and assign GigabitEthernet 1/0/5 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/5
[DeviceA-vlan10] quit
```

Create VLAN 20, and assign GigabitEthernet 1/0/6 to VLAN 20.

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/6
```

```
[DeviceA-vlan20] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 1. Configure Layer 2 aggregation group 1 to load share packets based on source MAC addresses.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation load-sharing mode source-mac
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to link aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an access port and assign it to VLAN 10.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port access vlan 10
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation1] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 2. Configure Layer 2 aggregation group 2 to load share packets based on destination MAC addresses.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation load-sharing mode destination-mac
[DeviceA-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to link aggregation group 2.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 2 as an access port and assign it to VLAN 20.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] port access vlan 20
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceA-Bridge-Aggregation2] quit
```

Configuring Device B

Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected , I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority  Oper-Key
  GE1/0/1(R)       S       32768     1
  GE1/0/2          S       32768     1

Aggregation Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority  Oper-Key
  GE1/0/3(R)       S       32768     2
  GE1/0/4          S       32768     2
```

The output shows that:

- Both link aggregation groups 1 and 2 load share traffic.
- Each aggregation group contains two Selected ports.

Display all the group-specific load sharing modes on Device A.

```
[DeviceA]display link-aggregation load-sharing mode interface Bridge-Aggregation 1
Bridge-Aggregation1 load-sharing mode:
source-mac address
[DeviceA]display link-aggregation load-sharing mode interface Bridge-Aggregation 2
Bridge-Aggregation2 load-sharing mode:
destination-mac address
```

The output shows that:

- Link aggregation group 1 distributes packets based on source MAC addresses.
- Link aggregation group 2 distributes packets based on destination MAC addresses.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 10
#
```

```
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 10
#
interface Bridge-Aggregation1
 port access vlan 10
 link-aggregation load-sharing mode source-mac
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 port link-aggregation group 1
#
interface Bridge-Aggregation2
 port access vlan 20
 link-aggregation load-sharing mode destination-mac
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 2
```

- Device B:

  The configuration file on Device B is the same as the configuration file on Device A.

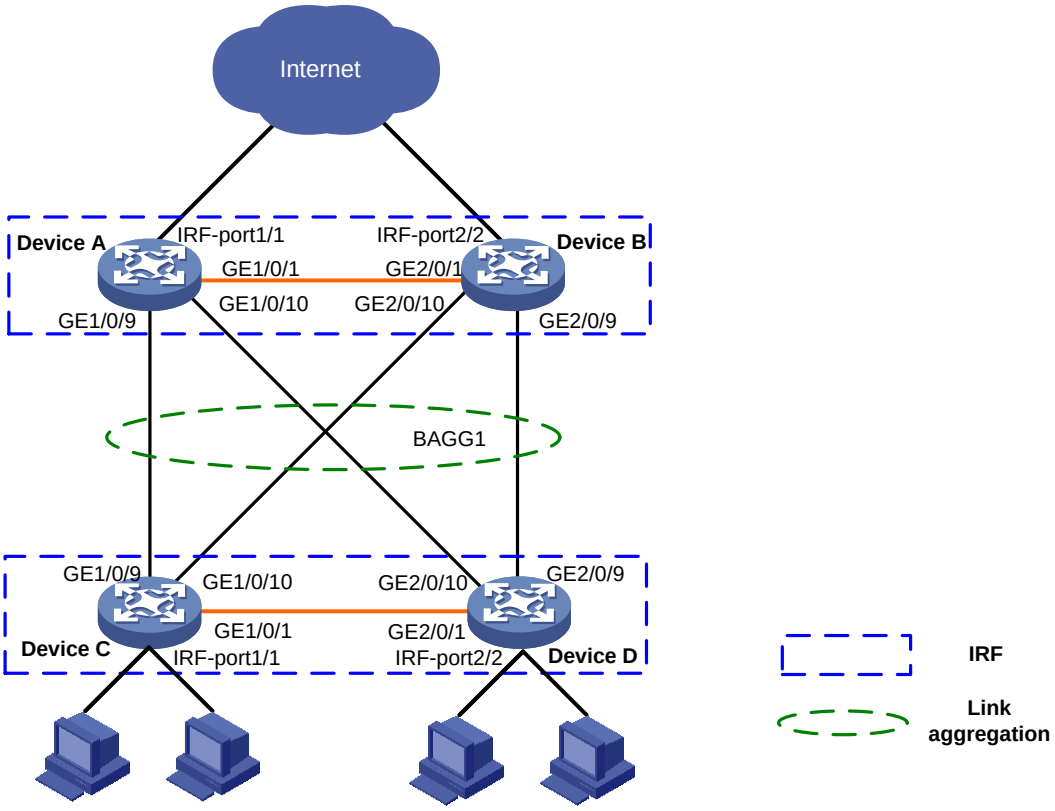
Example: Configuring Layer 2 link aggregation in an IRF fabric

Network configuration

On the network as shown in Figure 3, perform the following tasks:

- Set up a two-chassis IRF fabric at the access layer and a two-chassis IRF fabric at the distribution layer of the enterprise network.
- Configure link aggregation to improve the reliability of the links between the access-layer and distribution-layer IRF fabrics and implement load sharing.
- Run LACP MAD on the two IRF fabrics to detect IRF split.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series	Release 63xx

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure Layer 2 link aggregation in an IRF fabric, follow these restrictions and guidelines:

- IRF physical ports must be set to the bridge mode.
- When you bind physical ports to an IRF port, you must set all the physical ports to operate in either **normal** or **enhanced** mode.
- The physical ports of two connected IRF ports must operate in the same mode: **normal** or **enhanced**. For more information about the binding mode of the IRF physical ports, see *IRF Configuration Guide*.
- When you assign a port to an aggregation group, the recommended configuration procedure is as follows:
  a. Use the **`display this`** command in interface view to check the following attribute configurations of the port:
  - Port isolation.

- QinQ.
- VLAN.
- VLAN mapping.

b. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.

c. Assign the port to the aggregation group.

- In a static aggregation group, the Selected state of a port is not affected by whether the peer port is added to an aggregation group and is Selected. As a result, the Selected state of a port might be different from the Selected state of the peer port. When both ends support static aggregation and dynamic aggregation, use dynamic aggregation.
- You cannot assign a port to a Layer 2 aggregation group when MAC authentication, port security mode, or 802.1X is configured or enabled on the port.

Procedures

1. Configure IRF on Device A:

Shut down GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
[DeviceA-GigabitEthernet1/0/1] quit
```

Bind GigabitEthernet 1/0/1 to IRF port 1/1.

```
[DeviceA] irf-port 1/1
[DeviceA-irf-port1/1] port group interface gigabitethernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[DeviceA-irf-port1/1] quit
```

Bring up GigabitEthernet1/0/1, and save the configuration.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] save
```

Activate the IRF port configuration.

```
[DeviceA] irf-port-configuration active
```

2. Configure IRF on Device B:

Change the member ID of Device B to 2, and reboot the device to validate the change.

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

Shut down Gigabitethernet 2/0/1.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] shutdown
[DeviceB-GigabitEthernet2/0/1] quit
```

Bind GigabitEthernet 2/0/1 to IRF port 2/2.

```
[DeviceB] irf-port 2/2
[DeviceB-irf-port2/2] port group interface gigabitethernet 2/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[DeviceB-irf-port2/2] quit
```

Bring up GigabitEthernet 2/0/1, and save the configuration.

```
[DeviceB] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] undo shutdown
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] save
```

Activate the IRF port configuration.

```
[DeviceB] irf-port-configuration active
```

Device A and Device B perform master election, and the one that has lost the election reboots to form an IRF fabric with the master. In this example, Device B reboots.

Use the **`display irf`** command to verify that Device A has become the Master device.

```
[DeviceA] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master   1        00a0-fc00-5801  ---
   2        Standby  1        00e0-fc58-1235  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 00a0-fc00-5800
 Auto upgrade               : yes
 Mac persistent             : 6 min
 Domain ID                  : 0
 Auto merge                 : yes
```

3. Configure a Layer 2 aggregation group on Device A:

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the link aggregation mode as dynamic.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/9, GigabitEthernet1/0/10, GigabitEthernet 2/0/9, and GigabitEthernet 2/0/10 to link aggregation group 1.

```
[DeviceA] interface range gigabitethernet 1/0/9 to gigabitethernet 1/0/10
gigabitethernet 2/0/9 to gigabitethernet 2/0/10
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
[DeviceA]
```

Configure LACP MAD on the IRF fabric:

Set the domain ID of the IRF fabric to 1.

```
[DeviceA] irf domain 1
```

Enable LACP MAD on Bridge-Aggregation 1.

```
[DeviceA] interface Bridge-Aggregation 1
```

```
[DeviceA-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 1]:
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

4. Configure IRF on Device C in the same way IRF is configured on Device A. (Details not shown.)
5. Configure IRF on Device D in the same way IRF is configured on Device B. (Details not shown.)

   Device C and Device D perform master election, and the one that has lost the election reboots to form an IRF fabric with the master. In this example, Device C reboots.
6. Configure a Layer 2 dynamic aggregation group Bridge-Aggregation 1 on Device C in the same way Bridge-Aggregation 1 is configured on Device A. (Details not shown.)
7. Configure LACP MAD on the IRF fabric:

   # Set the domain ID of the IRF fabric to 2.

```
<DeviceC> system-view
[DeviceC] irf domain 2
```

   # Enable LACP MAD on Bridge-Aggregation 1.

```
[DeviceC] interface Bridge-Aggregation 1
[DeviceC-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 2]:
The assigned domain ID is: 2
MAD LACP only enable on dynamic aggregation interface.
```

Verifying the configuration

Display the information about the link aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 00a0-fc00-5800
Local:
  Port                Status   Priority Index    Oper-Key              Flag
  GE1/0/9(R)          S        32768    10       1                     {ACG}
  GE1/0/10            S        32768    11       1                     {ACG}
  GE2/0/9             S        32768    138      1                     {ACG}
  GE2/0/10            S        32768    139      1                     {ACG}
Remote:
  Actor               Priority Index    Oper-Key SystemID              Flag
```

```
GE1/0/9             32768    0        0        0x8000, 0000-0000-0000 {EF}
GE1/0/10            32768    0        0        0x8000, 0000-0000-0000 {EF}
GE2/0/9             32768    0        0        0x8000, 0000-0000-0000 {EF}
GE2/0/10            32768    0        0        0x8000, 0000-0000-0000 {EF}
```

The output shows that the local member ports and the corresponding peer member ports are all Selected. In the dynamic link aggregation mode, each local member port and its peer member port have the same Selected state through exchanging LACPDUs. The user data traffic can be forwarded correctly.

Shut down physical IRF port GigabitEthernet 2/0/1 on Device B.

A log message appears on Device A.

```
[DeviceA]%Jul  9 16:52:41:734 2016 DeviceA STM/3/STM_LINK_DOWN: IRF port 1 went down.
%Jul  9 16:52:41:800 2016 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to down.
%Jul 9 16:52:41:854 2016 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface
GigabitEthernet1/0/1 changed to down.
%Jul 9 16:52:41:867 2016 DeviceA DEV/3/BOARD_REMOVED: Board was removed from slot 2, type
is Simware.
```

The output shows that IRF split occurs on the distribution layer because GigabitEthernet 2/0/1 that is bound to IRF port 2/2 is physically down.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 irf domain 1
 irf mac-address persistent timer
 irf auto-update enable
 irf auto-merge enable
 undo irf link-delay
 irf member 1 priority 1
 irf member 2 priority 1
#
irf-port 1/1
 port group interface GigabitEthernet1/0/1
#
irf-port 2/2
 port group interface GigabitEthernet2/0/1
#

interface Bridge-Aggregation1
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/9
 port link-mode bridge
 port link-aggregation group 1
```

```
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port link-aggregation group 1
#
interface GigabitEthernet2/0/9
 port link-mode bridge
 port link-aggregation group 1
#
interface GigabitEthernet2/0/10
 port link-mode bridge
 port link-aggregation group 1
#
```

- Device C:

  The configuration file on Device C is similar as the configuration file on Device A.

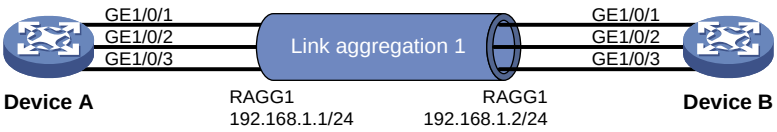
Example: Configuring Layer 3 link aggregation

Network configuration

On the network as shown in Figure 4, perform the following tasks:

- Configure a Layer 3 dynamic aggregation group on both Device A and Device B.
- Configure IP addresses and subnet masks for the corresponding Layer 3 aggregate interfaces.

Figure 4 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx,

	Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx

S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

In a static aggregation group, the Selected state of a port is not affected by whether the peer port is added to an aggregation group and is Selected. As a result, the Selected state of a port might be different from the Selected state of the peer port. When both ends support static aggregation and dynamic aggregation, use dynamic aggregation.

If you use the S5570S-EI, S5500V3-SI, S3600V3-EI, or S3600V3-SI switch series, reserve local VLAN interface resources by using the **`reserve-vlan-interface`** command before you switch Layer 2 Ethernet interfaces to Layer 3 Ethernet interfaces or create Layer 3 aggregate interfaces. For more information about VLAN interface resource reservation, see the VLAN configuration and commands for the products.

Procedures

1. Configure Device A:

Create Layer 3 aggregate interface Route-Aggregation 1. Use one of the following methods as needed.

- Use the static aggregation mode to create Layer 3 aggregate interface Route-Aggregation 1.

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
```

- Use the dynamic aggregation mode to create Layer 3 aggregate interface Route-Aggregation 1.

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
[DeviceA-Route-Aggregation1] link-aggregation mode dynamic
```

Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 1.

```
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] undo shutdown
[DeviceA-Route-Aggregation1] quit
```

Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 1.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-mode route
[DeviceA-if-range] undo shutdown
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about the link aggregation groups on Device A.

- Link aggregation configuration information when the static aggregation mode is used:

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
  GE1/0/3          S       32768    1
```

The output shows that all member ports in the local aggregation group are in Selected state. The Selected states of the local member ports are not affected by the Selected states of the peer member ports.

- Link aggregation configuration information when the dynamic aggregation mode is used:

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    2        1                      {ACDEF}
  GE1/0/2             S        32768    3        1                      {ACDEF}
  GE1/0/3             S        32768    4        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    2        1        0x8000, 68fa-34f2-0200 {ACDEF}
  GE1/0/2             32768    3        1        0x8000, 68fa-34f2-0200 {ACDEF}
  GE1/0/3             32768    4        1        0x8000, 68fa-34f2-0200 {ACDEF}
```

The output shows that the local member ports and the corresponding peer member ports are all Selected. In the dynamic link aggregation mode, each local member port and its peer member port have the same Selected state through exchanging LACPDUs. The user data traffic can be forwarded correctly.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

  ```
  #
  ```

  - In the static aggregation mode:

    ```
    #
    interface route-aggregation1
     ip address 192.168.1.1 255.255.255.0
    #
    ```

  - In the dynamic aggregation mode:

    ```
    #
    interface route-aggregation1
     ip address 192.168.1.1 255.255.255.0
     link-aggregation mode dynamic
    #
    interface GigabitEthernet1/0/1
    ```

```
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode route
 port link-aggregation group 1
#
 Device B:
```

The configuration file on Device B is similar as the configuration file on Device A.

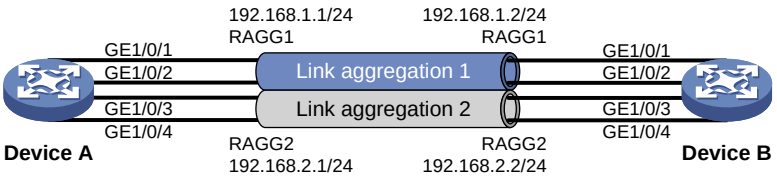
Example: Configuring Layer 3 aggregation load sharing

Network configuration

As shown in Figure 5, configure link aggregation on Device A and Device B to meet the following requirements:

- Configure Layer 3 static aggregation groups 1 and 2 on both Device A and Device B.
- Assign IP addresses and subnet masks to the Layer 3 aggregate interfaces of the aggregation groups.
- Configure link aggregation groups 1 and 2 to load share traffic across aggregation group member ports.
  - Configure link aggregation group 1 to load share packets based on source IP addresses.
  - Configure link aggregation group 2 to load share packets based on destination IP addresses.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported

S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported

S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

You can set the global or group-specific load sharing mode. A link aggregation group preferentially uses the group-specific load sharing mode. If the group-specific load sharing mode is not available, the group uses the global load sharing mode. This example uses group-specific load sharing mode configuration.

Procedures

Configuring Device A

Create Layer 3 aggregate interface Route-Aggregation 1.

```
<DeviceA> system-view
[DeviceA] interface route-aggregation 1
```

Configure Layer 3 aggregation group 1 to load share packets based on source IP addresses.

```
[DeviceA-Route-Aggregation1] link-aggregation load-sharing mode source-ip
```

Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 1.

```
[DeviceA-Route-Aggregation1] ip address 192.168.1.1 24
[DeviceA-Route-Aggregation1] quit
```

Create Layer 3 aggregate interface Route-Aggregation 2.

```
[DeviceA] interface route-aggregation 2
```

Configure Layer 3 aggregation group 2 to load share packets based on destination IP addresses.

```
[DeviceA-Route-Aggregation2] link-aggregation load-sharing mode destination-ip
```

Configure an IP address and subnet mask for Layer 3 aggregate interface Route-Aggregation 2.

```
[DeviceA-Route-Aggregation2] ip address 192.168.2.1 24
[DeviceA-Route-Aggregation2] quit
```

Assign Layer 3 Ethernet interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.

```
[DeviceA] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceA-if-range] port link-mode route
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] quit
```

Assign Layer 3 Ethernet interfaces GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 2.

```
[DeviceA] interface range gigabitethernet 1/0/3 gigabitethernet 1/0/4
[DeviceA-if-range] port link-mode route
[DeviceA-if-range] port link-aggregation group 2
[DeviceA-if-range] quit
```

Configuring Device B

Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display detailed information about all aggregation groups on Device A.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/1(R)       S       32768    1
  GE1/0/2          S       32768    1
```

```
Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/3(R)       S       32768    2
  GE1/0/4          S       32768    2
```

The output shows that:

- Both link aggregation groups 1 and 2 load share traffic.
- Each aggregation group contains two Selected ports.

Display all the group-specific load sharing modes on Device A.

```
[DeviceA] display link-aggregation load-sharing mode interface
Route-Aggregation1 load-sharing mode:
source-ip address

Route-Aggregation2 load-sharing mode:
destination-ip address
```

The output shows that:

- Link aggregation group 1 distributes packets based on source IP addresses.
- Link aggregation group 2 distributes packets based on destination IP addresses.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
interface Route-Aggregation1
 ip address 192.168.1.1 255.255.255.0
 link-aggregation load-sharing mode source-ip
#
interface Route-Aggregation2
 ip address 192.168.2.1 255.255.255.0
 link-aggregation load-sharing mode destination-ip
#
interface GigabitEthernet1/0/1
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode route
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
```

```
 port link-mode route
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port link-mode route
 port link-aggregation group 2
#
```

- Device B:

  The configuration file on Device B is similar to the configuration file on Device A.

Contents

Introduction

This document provides port isolation configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of port isolation.

General restrictions and guidelines

You cannot assign the member ports of a service loopback group to an isolation group. You cannot assign the member ports of an isolation group to a service loopback group.

Example: Configuring port isolation

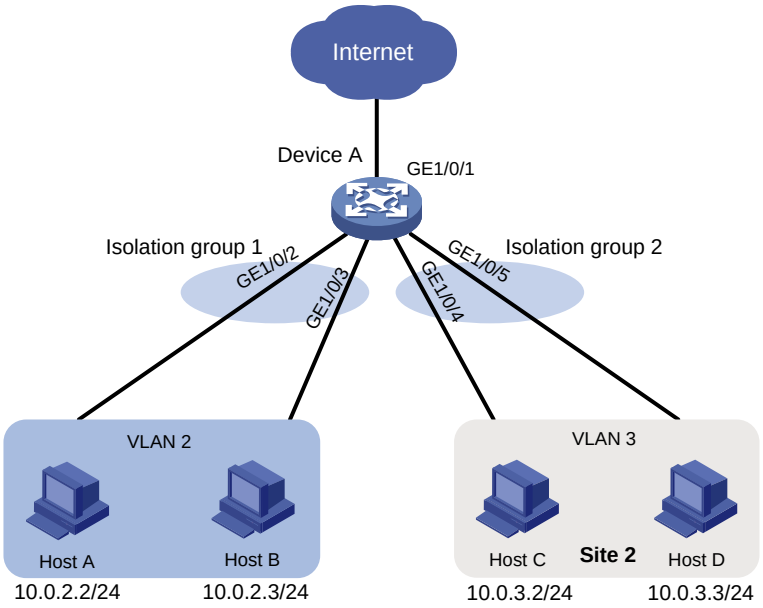
Network configuration

As shown in Figure 1, the company branches Site 1 and Site 2 transfer service traffic in VLAN 2 and VLAN 3. Device A connects to the Internet through GigabitEthernet 1/0/1.

Configure port isolation on Device A to meet the following requirements:

- All hosts can access the Internet through Device A.
- Host A and Host B are isolated from each other at Layer 2.
- Host C and Host D are isolated from each other at Layer 2.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch	Release 63xx

Hardware	Software version
E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure port isolation on the device, follow these restrictions and guidelines:

- Before assigning a port to an isolation group, make sure the isolation group already exists.
- You can assign a port to only one isolation group.

Procedures

Create VLAN 2 and assign ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to the VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] port gigabitethernet 1/0/3
[DeviceA-vlan2] quit
```

Create VLAN 3 and assign ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5 to the VLAN.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/4
[DeviceA-vlan3] port gigabitethernet 1/0/5
[DeviceA-vlan3] quit
```

Configure port GigabitEthernet 1/0/1 as a trunk port and assign it to VLAN 2 and VLAN 3.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 3
[DeviceA-GigabitEthernet1/0/1] quit
```

Create isolation groups 1 and 2.

```
[DeviceA] port-isolate group 1
[DeviceA] port-isolate group 2
```

Assign ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to isolation group 1.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port-isolate enable group 1
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port-isolate enable group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Assign ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5 to isolation group 2.

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port-isolate enable group 2
[DeviceA-GigabitEthernet1/0/4] quit
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port-isolate enable group 2
[DeviceA-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display information about all isolation groups.

```
[DeviceA] display port-isolate group
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3

Group ID: 2
 Group members:
    GigabitEthernet1/0/4
    GigabitEthernet1/0/5
```

The output shows that:

- Ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are in isolation group 1. As a result, Host A and Host B are isolated from each other at Layer 2.
- Ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/4 are in isolation group 2. As a result, Host C and Host D are isolated from each other at Layer 2.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 port-isolate group 1
 port-isolate group 2
#
```

```
vlan 2 to 3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
 port-isolate enable group 1
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 port-isolate enable group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 3
 port-isolate enable group 2
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 3
 port-isolate enable group 2
#
```

Contents

Introduction

This document provides spanning tree configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of spanning tree protocols.

Example: Configuring MSTP

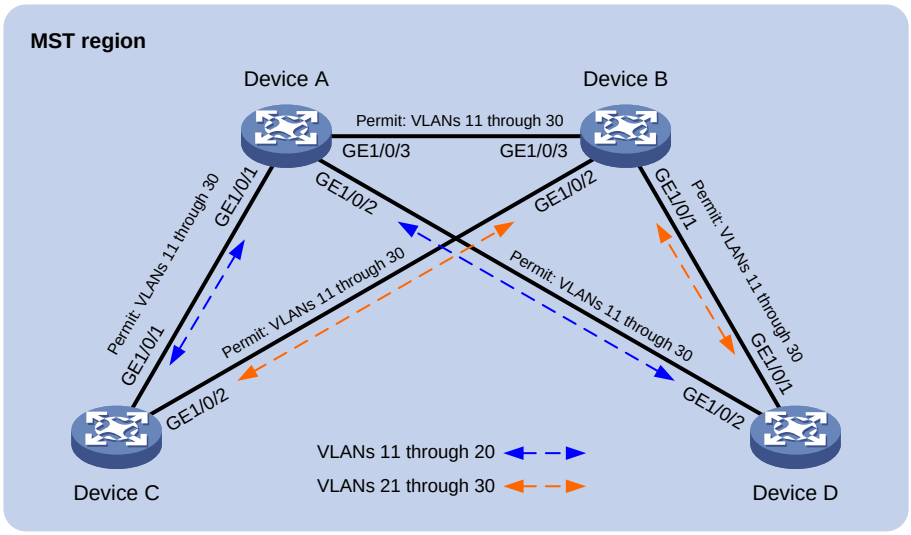
Network configuration

As shown in Figure 1, Device A and Device B operate at the core layer, and Device C and Device D operate at the distribution layer. The ports on the devices have the same path cost, and they all permit VLANs 11 through 30.

Configure MSTP to meet the following requirements:

- Device A, Device B, Device C, and Device D belong to the same MST region.
- MSTIs are used to share the traffic of VLANs 11 through 20 and of VLANs 21 through 30.

Figure 1 Network diagram



Analysis

To assign the devices to the same MST region, make sure the following MST region parameters are the same on the devices:

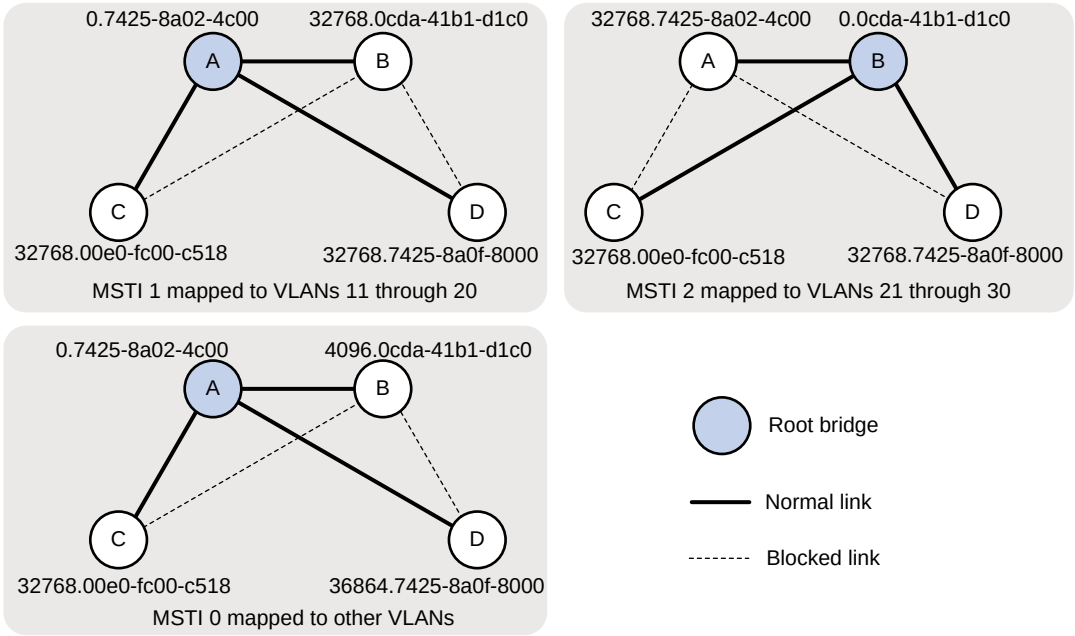
- Spanning tree mode (the default mode MSTP is used).

- Region name (**test** in this example).
- Revision level (the default value 0 is used).
- VLAN-to-instance mappings (VLANs 11 through 20 to MIST 1, and VLANs 21 through 30 to MIST 2).

To use redundant links to share the traffic of different VLANs (as shown in Figure 2), perform the following tasks:

- Configure Device A as the root bridge of MSTI 1.
- Configure Device B as the root bridge of MIST 2.
- Assign priorities to Device A, Device B, Device C, and Device D in MSTI 0 in descending order for Device A to be the regional root bridge.

Figure 2 MSTIs mapped to different VLANs



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI switch)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx

Hardware	Software version
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Device A

Create VLANs 11 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 11 to 30
```

Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to trunk VLANs 11 through 30.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-type trunk
[DeviceA-if-range] port trunk permit vlan 11 to 30
[DeviceA-if-range] quit
```

Configure the MST region name as **test**.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1, and map VLANs 21 through 30 to MSTI 2.

```
[DeviceA-mst-region] instance 1 vlan 11 to 20
[DeviceA-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure Device A as the root bridge of MSTI 0 and MSTI 1.

```
[DeviceA] stp instance 0 to 1 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create VLANs 11 through 30.

```
<DeviceB> system-view
[DeviceB] vlan 11 to 30
```

Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to trunk VLANs 11 through 30.

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceB-if-range] port link-type trunk
[DeviceB-if-range] port trunk permit vlan 11 to 30
[DeviceB-if-range] quit
```

Configure the MST region name as **test**.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1, and map VLANs 21 through 30 to MSTI 2.

```
[DeviceB-mst-region] instance 1 vlan 11 to 20
[DeviceB-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure Device B as the root bridge of MSTI 2 and a secondary root bridge of MSTI 0.

```
[DeviceB] stp instance 2 root primary
[DeviceB] stp instance 0 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring Device C

Create VLANs 11 through 30.

```
<DeviceC> system-view
[DeviceC] vlan 11 to 30
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to trunk VLANs 11 through 30.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-type trunk
[DeviceC-if-range] port trunk permit vlan 11 to 30
```

```
[DeviceC-if-range] quit
```

Configure the MST region name as **test**.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name test
```

Map VLANs 11 through 20 through MSTI 1, and map VLANs 21 through 30 to MSTI 2.

```
[DeviceC-mst-region] instance 1 vlan 11 to 20
[DeviceC-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Enable the spanning tree feature globally.

```
[DeviceC] stp global enable
```

Configuring Device D

Create VLANs 11 through 30.

```
<DeviceD> system-view
[DeviceD] vlan 11 to 30
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to trunk VLANs 11 through 30.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-type trunk
[DeviceD-if-range] port trunk permit vlan 11 to 30
[DeviceD-if-range] quit
```

Configure the MST region name as **test**.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1, and map VLANs 21 through 30 to MSTI 2.

```
[DeviceD-mst-region] instance 1 vlan 11 to 20
[DeviceD-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Set the device priority to 36864 in MSTI 0, which is lower than the default priority 32768 of Device C.

```
[DeviceD] stp instance 0 priority 36864
```

Enable the spanning tree feature globally.

```
[DeviceD] stp global enable
```

Verifying the configuration

1. Verify that Layer 2 loops have been eliminated in each MSTI:

   Use the **`display stp brief`** command to display brief spanning tree information on each device.

   # Display brief spanning tree information on Device A.

   ```
   [DeviceA] display stp brief
    MST ID   Port                                    Role  STP State   Protection
   ```

```
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
```

Display brief spanning tree information on Device C.

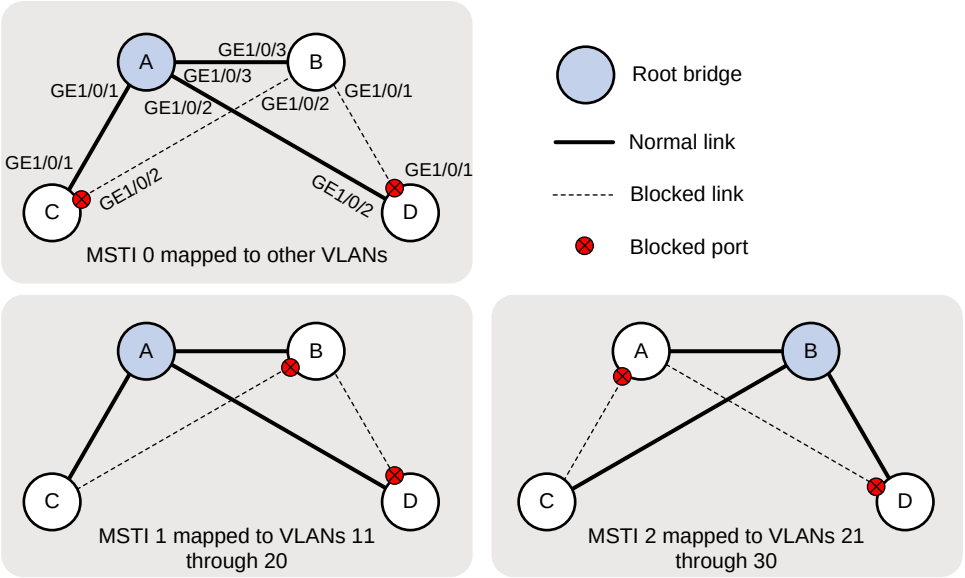
```
[DeviceC] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/1                    ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/1                    ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    ALTE  DISCARDING  NONE
 0        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                    ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                    ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    ALTE  DISCARDING  NONE
```

Based on the output, the topology for each MSTI is shown in Figure 3.

Figure 3 MSTI topologies



2. Verify that the network can accommodate topology changes:

Shut down GigabitEthernet 1/0/1 on Device C. (Details not shown.)

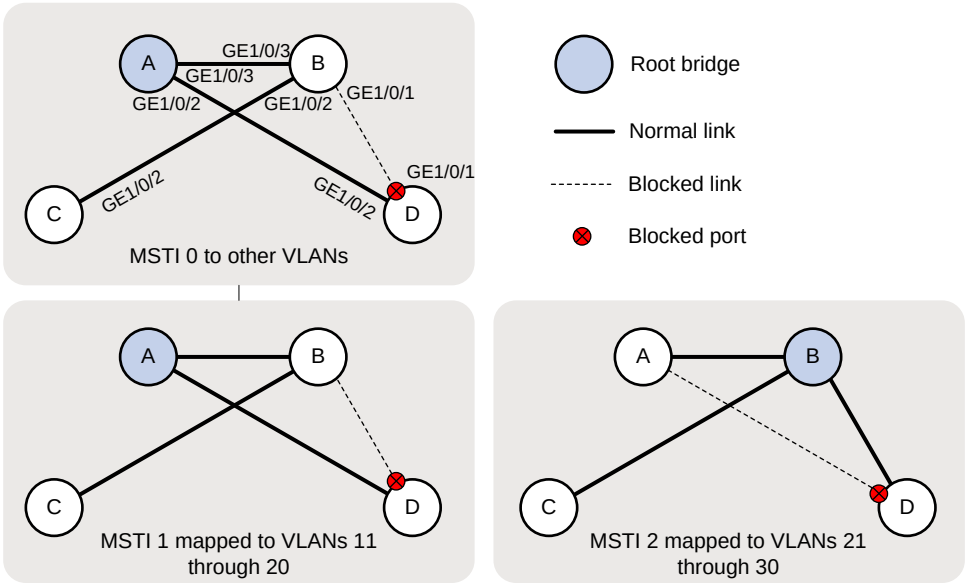
Display brief spanning tree information on all devices.

```
[DeviceA] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
[DeviceB] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                    ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
[DeviceC] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
[DeviceD] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    ALTE  DISCARDING  NONE
```

```
0          GigabitEthernet1/0/2                    ROOT   FORWARDING   NONE
1          GigabitEthernet1/0/1                    ALTE   DISCARDING   NONE
1          GigabitEthernet1/0/2                    ROOT   FORWARDING   NONE
2          GigabitEthernet1/0/1                    ROOT   FORWARDING   NONE
2          GigabitEthernet1/0/2                    ALTE   DISCARDING   NONE
```

Based on the output, the topology for each MSTI is shown in Figure 4.

Figure 4 MSTI topologies



Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 to 1 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
```

- Device B:

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 root secondary
 stp instance 2 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
```

- Device C:

```
#
vlan 1
#
```

```
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
```

- Device D:

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 priority 36864
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
```

Example: Configuring PVST

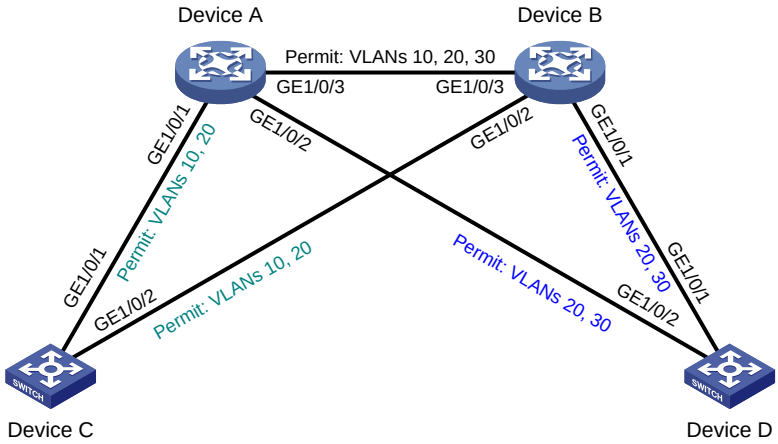
Network configuration

As shown in Figure 5, Device A and Device B operate at the distribution layer, and Device C and Device D operate at the access layer. The ports on the devices have the same path cost.

Configure PVST to meet the following requirements:

- Redundant links are used for load sharing.
- Packets of each VLAN are forwarded along its spanning tree.

Figure 5 Network diagram

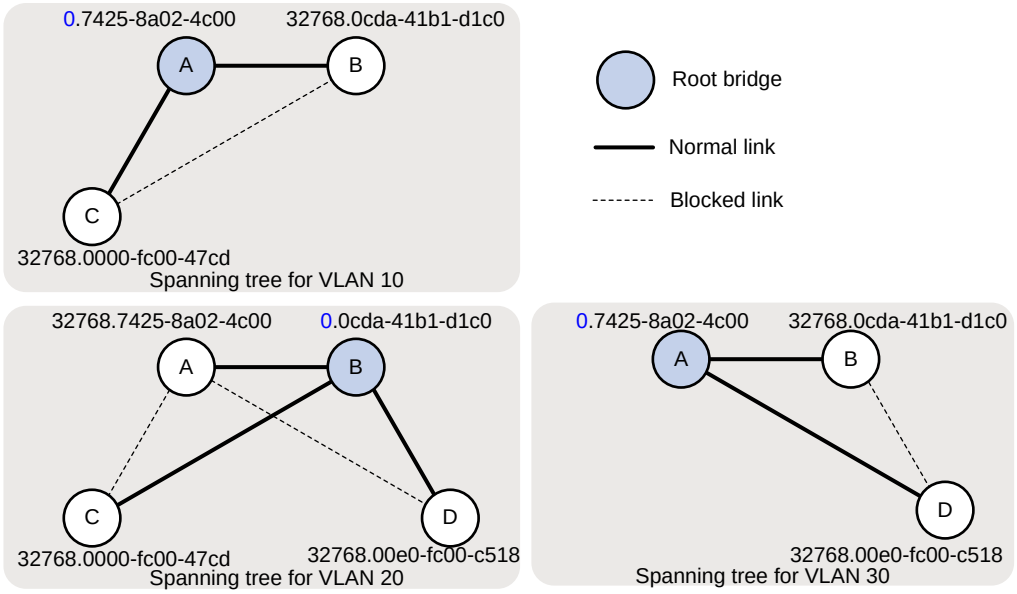


Analysis

For traffic of different VLANs to be shared along the spanning trees in Figure 6, perform the following tasks:

- Configure Device A as the root bridge of the spanning trees for VLAN 10 and VLAN 30.
- Configure Device B as the root bridge of the spanning tree for VLAN 20.

Figure 6 VLAN spanning tree topologies



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI switch)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series	Release 63xx

Hardware	Software version
E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Device A

Create VLAN 10, VLAN 20, and VLAN 30.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] vlan 20
[DeviceA-vlan20] vlan 30
[DeviceA-vlan30] quit
```

Configure GigabitEthernet 1/0/1 to trunk VLAN 10 and VLAN 20.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 to trunk VLAN 20 and VLAN 30.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 20 30
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 to trunk VLAN 10, VLAN 20, and VLAN 30.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10 20 30
[DeviceA-GigabitEthernet1/0/3] quit
```

Set the spanning tree mode to PVST.

```
[DeviceA] stp mode pvst
```

Configure Device A as the root bridge of VLAN 10 and VLAN 30.

```
[DeviceA] stp vlan 10 30 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create VLAN 10, VLAN 20, and VLAN 30.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] vlan 20
[DeviceB-vlan20] vlan 30
[DeviceB-vlan30] quit
```

Configure GigabitEthernet 1/0/1 to trunk VLAN 20 and VLAN 30.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 30
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 to trunk VLAN 10 and VLAN 20.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 to trunk VLAN 10, VLAN 20, and VLAN 30.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10 20 30
[DeviceB-GigabitEthernet1/0/3] quit
```

Set the spanning tree mode to PVST.

```
[DeviceB] stp mode pvst
```

Configure Device B as the root bridge of VLAN 20.

```
[DeviceB] stp vlan 20 root primary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring Device C

Create VLAN 10 and VLAN 20.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] vlan 20
[DeviceC-vlan20] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to trunk VLAN 10 and VLAN 20.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-type trunk
```

```
[DeviceC-if-range] port trunk permit vlan 10 20
[DeviceC-if-range] quit
```

Set the spanning tree mode to PVST.

```
[DeviceC] stp mode pvst
```

Enable the spanning tree feature globally.

```
[DeviceC] stp global enable
```

Configuring Device D

Create VLAN 20 and VLAN 30.

```
<DeviceD> system-view
[DeviceD] vlan 20
[DeviceD-vlan20] vlan 30
[DeviceD-vlan30] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to trunk VLAN 20 and VLAN 30.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-type trunk
[DeviceD-if-range] port trunk permit vlan 20 30
[DeviceD-if-range] quit
```

Set the spanning tree mode to PVST.

```
[DeviceD] stp mode pvst
```

Enable the spanning tree feature globally.

```
[DeviceD] stp global enable
```

Verifying the configuration

Use the **`display stp brief`** command to display brief spanning tree information on each device.

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 VLAN ID  Port                                Role  STP State   Protection
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                ALTE  DISCARDING  NONE
 10       GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 10       GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 20       GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 20       GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 20       GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
 30       GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 30       GigabitEthernet1/0/3                DESI  FORWARDING  NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 VLAN ID  Port                                Role  STP State   Protection
 1        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

```
 1        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 10       GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 10       GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
 20       GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 20       GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 20       GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 30       GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 30       GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
```

Display brief spanning tree information on Device C.

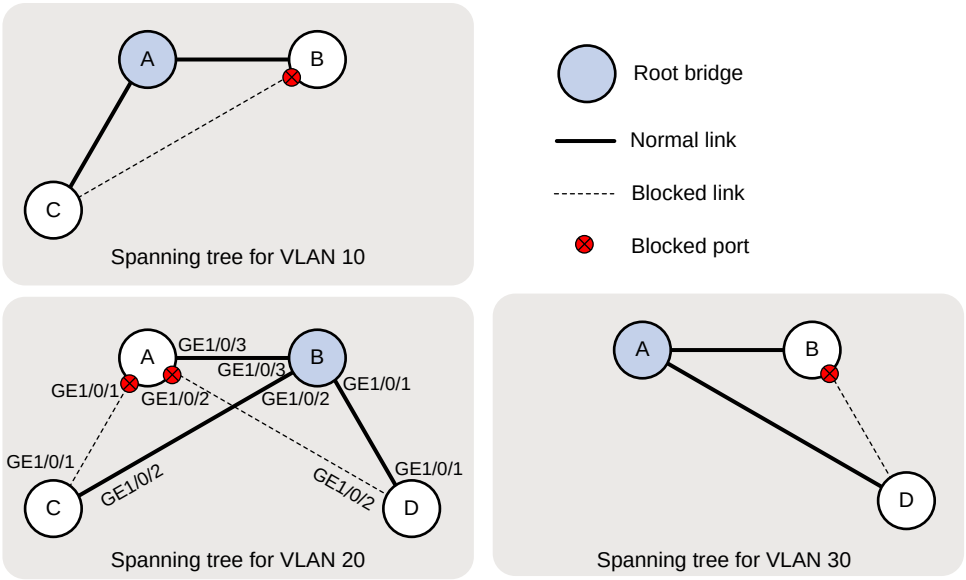
```
[DeviceC] display stp brief
 VLAN ID  Port                                Role  STP State   Protection
 1        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 10       GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 10       GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 20       GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 20       GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 VLAN ID  Port                                Role  STP State   Protection
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 20       GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 20       GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 30       GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 30       GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

Based on the output, the topology for each VLAN is shown in Figure 7.

Figure 7 VLAN spanning tree topologies



Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 30
#
 stp vlan 10 30 root primary
 stp mode pvst
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 20 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20 30
#
```

- Device B:

```
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 30
#
 stp vlan 20 root primary
 stp mode pvst
 stp global enable
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 20 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20 30
#
```

- Device C:

```
#
vlan 1
#
vlan 10
#
vlan 20
#
 stp mode pvst
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
#
```

- Device D:

```
#
vlan 1
#
vlan 20
#
vlan 30
#
 stp mode pvst
 stp global enable
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 20 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 20 30
#
```

Example: Configuring RSTP

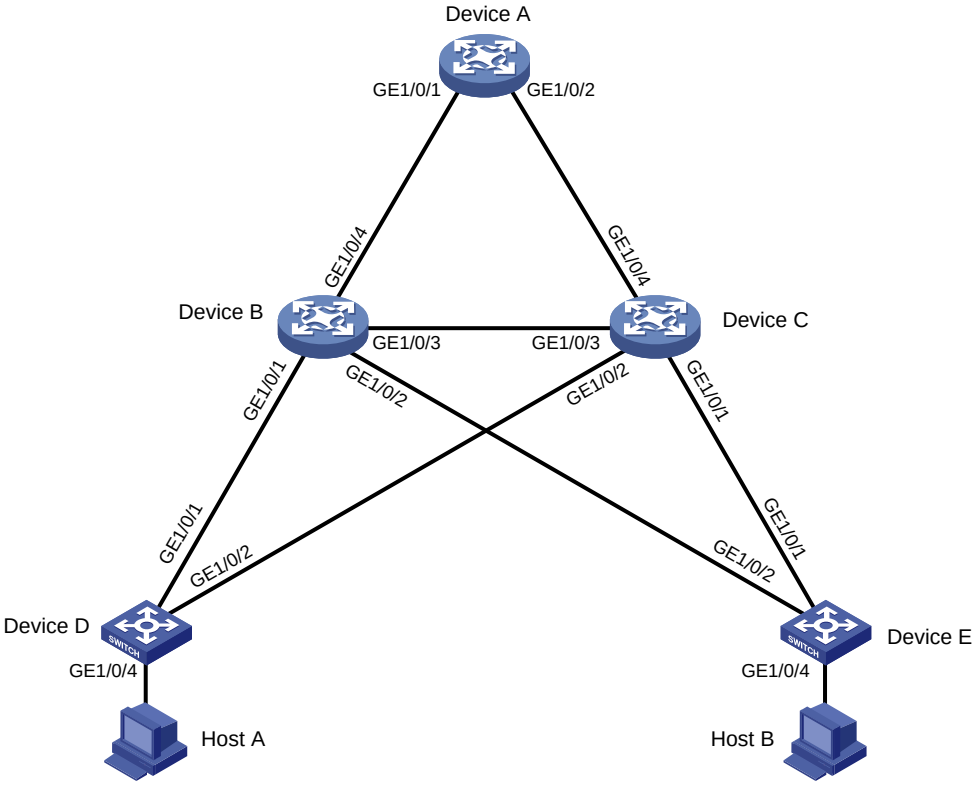
Network configuration

As shown in Figure 8, Device A operates at the core layer, Device B and Device C operate at the distribution layer, and Device D and Device E operate at the access layer. The ports on the devices have the same path cost.

Configure RSTP as follows:

- Configure Device A as the root bridge, and enable root guard to retain its root bridge role when configuration errors or malicious attacks occur.
- Configure Device C as a backup of Device B. When Device B fails, traffic is forwarded through Device C.
- Configure GigabitEthernet 1/0/4 on Device D and GigabitEthernet 1/0/4 on Device E as edge ports, and enable BPDU guard on the ports.

Figure 8 Network diagram



Analysis

For Device C to be a backup of Device B, make sure Device C's priority is lower than Device B's priority. In this example, configure the priorities of Device B and Device C as 4096 and 8192.

For Device A to be the root bridge, make sure Device A has the lowest bridge ID (containing the device's priority and MAC address) in the network. In this example, because Device A already has the lowest MAC address, configure the priority as 4096 for Device A to hold the lowest bridge ID.

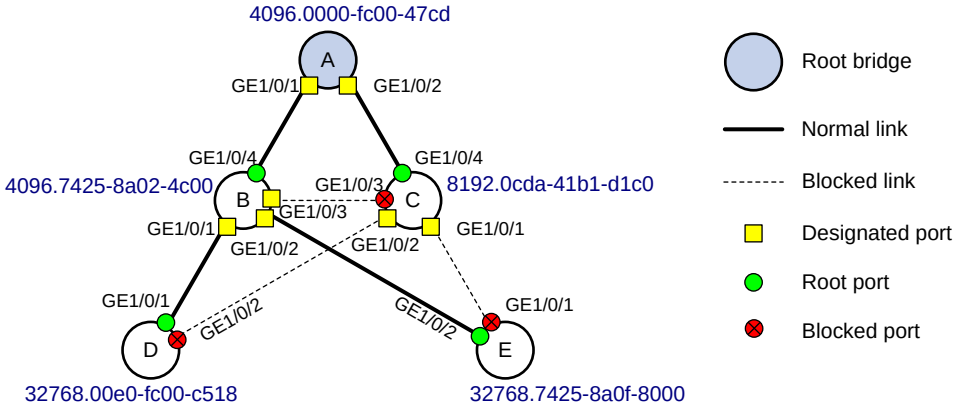
NOTE:

To configure a device as the root bridge, you also can use the **`stp root primary`** or **`stp priority 0`** command to set the device's priority to 0.

To retain Device A's root bridge role, enable root guard on the designated ports of Device A, Device B, and Device C. To identify the designated ports, use either of the following methods:

- Use the **`display stp brief`** command to display the brief spanning tree information. The role is **DESI** for a designated port.
- Identify the designated ports in the RSTP topology that is calculated based on the device configuration, as shown in Figure 9.

Figure 9 RSTP topology



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx,

Hardware	Software version
	Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI switch)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series	Release 63xx

Hardware	Software version
MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Device A

Set the spanning tree mode to RSTP.

```
<DeviceA> system-view
[DeviceA] stp mode rstp
```

Configure the priority as 4096 for Device A.

```
[DeviceA] stp priority 4096
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Enable root guard on designated ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceA-if-range] stp root-protection
[DeviceA-if-range] quit
```

Configuring Device B

Set the spanning tree mode to RSTP.

```
<DeviceB> system-view
[DeviceB] stp mode rstp
```

Configure the priority as 4096 for Device B.

```
[DeviceB] stp priority 4096
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Enable root guard on designated ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceB-if-range] stp root-protection
[DeviceB-if-range] quit
```

Configuring Device C

Set the spanning tree mode to RSTP.

```
<DeviceC> system-view
[DeviceC] stp mode rstp
```

Configure the priority as 8192 for Device C.

```
[DeviceC] stp priority 8192
```

Enable the spanning tree feature globally.

```
[DeviceC] stp global enable
```

Enable root guard on designated ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] stp root-protection
[DeviceC-if-range] quit
```

Configuring Device D

Set the spanning tree mode to RSTP.

```
<DeviceD> system-view
[DeviceD] stp mode rstp
```

Enable the spanning tree feature globally.

```
[DeviceD] stp global enable
```

Configure GigabitEthernet 1/0/4 as an edge port, and enable BPDU guard.

```
[DeviceD] interface gigabitethernet 1/0/4
[DeviceD-GigabitEthernet1/0/4] stp edged-port
[DeviceD-GigabitEthernet1/0/4] quit
[DeviceD] stp bpdu-protection
```

Configuring Device E

Configure Device E in the same way you configure Device D. (Details not shown.)

Verifying the configuration

1. Verify that Layer 2 loops have been eliminated in the network:

   Use the **`display stp brief`** command to display brief spanning tree information on each device.

   # Display the brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
```

   # Display the brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  NONE
```

```
 0         GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 0         GigabitEthernet1/0/4                ROOT  FORWARDING  NONE
```

Display the brief spanning tree information on Device C.

```
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0         GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 0         GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 0         GigabitEthernet1/0/3                ALTE  DISCARDING  NONE
 0         GigabitEthernet1/0/4                ROOT  FORWARDING  NONE
```

Display the brief spanning tree information on Device D.

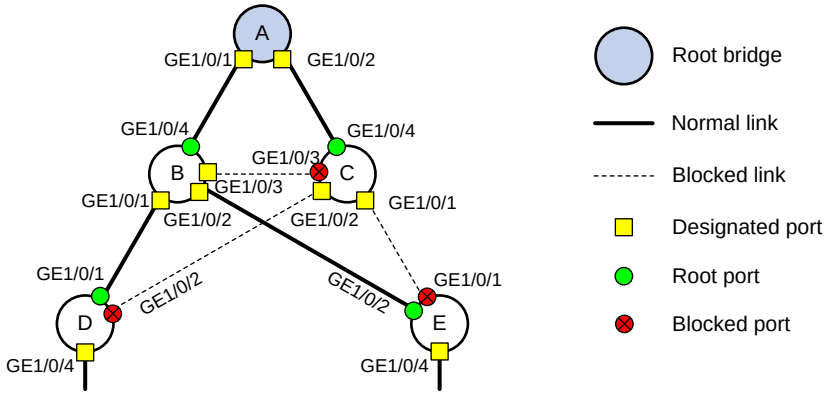
```
[DeviceD] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0         GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 0         GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 0         GigabitEthernet1/0/4                DESI  FORWARDING  BPDU
```

Display the brief spanning tree information on Device E.

```
[DeviceE] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0         GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 0         GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 0         GigabitEthernet1/0/4                DESI  FORWARDING  BPDU
```

Based on the output, the topology for the network is shown in Figure 10.

Figure 10 Network topology



2. Verify that root guard can retain Device A's root bridge role:

Verify that Device A is the root bridge in the network.

```
[DeviceD] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 32768.00e0-fc00-c518
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 4096.0000-fc00-47cd, 40
 RegRoot ID/IRPC     : 32768.00e0-fc00-c518, 0
...
```

Set the priority to 0 for Device D. Because the priority is higher than the priority of Device A, Device D considers itself as the root bridge and sends BPDUs that contain its bridge ID 0.00e0-fc00-c518.

```
[DeviceD] stp priority 0
```

```
[DeviceD] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 0.00e0-fc00-c518
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 0.00e0-fc00-c518, 0
 RegRoot ID/IRPC     : 0.00e0-fc00-c518, 0
...
```

Set the priority to 0 for Device E. Because the priority is higher than the priority of Device A. Device E considers itself as the root bridge and sends BPDUs that contain its bridge ID 0.7425-8a0f-8000.

```
[DeviceE] stp priority 0
[DeviceE] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 0.7425-8a0f-8000
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 0.7425-8a0f-8000, 0
 RegRoot ID/IRPC     : 0.7425-8a0f-8000, 0
...
```

Verify that Device A is still the root bridge in the network. The ports connected Device B and Device C to Device D and Device E transit to the discarding state.

```
[DeviceB] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 4096.7425-8a02-4c00
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 4096.0000-fc00-47cd, 20
 RegRoot ID/IRPC     : 4096.7425-8a02-4c00, 0
...
[DeviceC] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 8192.0cda-41b1-d1c0
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 4096.0000-fc00-47cd, 20
 RegRoot ID/IRPC     : 8192.0cda-41b1-d1c0, 0
...
[DeviceB] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        Ten-GigabitEthernet1/0/1            DESI  DISCARDING  NONE
 0        Ten-GigabitEthernet1/0/2            DESI  DISCARDING  NONE
 0        Ten-GigabitEthernet1/0/3            DESI  FORWARDING  NONE
 0        Ten-GigabitEthernet1/0/4            ROOT  FORWARDING  NONE
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        Ten-GigabitEthernet1/0/1            DESI  DISCARDING  NONE
 0        Ten-GigabitEthernet1/0/2            DESI  DISCARDING  NONE
 0        Ten-GigabitEthernet1/0/3            ALTE  DISCARDING  NONE
 0        Ten-GigabitEthernet1/0/4            ROOT  FORWARDING  NONE
```

Verify that Device A cannot retain its root bridge role when root guard is disabled on a designated port on Device B (for example, GigabitEthernet 1/0/2).

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] undo stp root-protection
[DeviceB-GigabitEthernet1/0/2] display stp
-------[CIST Global Info] [Mode RSTP] -------
 Bridge ID           : 4096.7425-8a02-4c00
 Bridge times        : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC        : 0.7425-8a0f-8000, 20
...
[DeviceB-GigabitEthernet1/0/2] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  DISCARDING  ROOT
 0        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/3                    DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/4                    DESI  FORWARDING  NONE
```

3. Verify that traffic is forwarded through Device C when Device B fails:

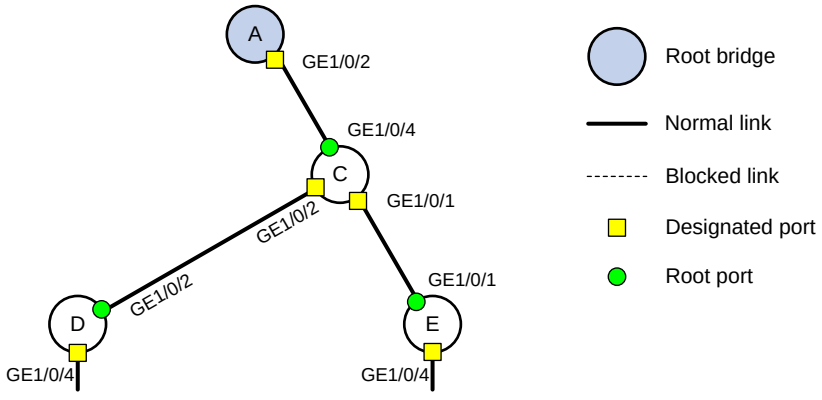
Reboot Device B. (Details not shown.)

Display the brief spanning tree information on Device A, Device C, Device D, and Device E before Device B completes the reboot.

```
[DeviceA] dis stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  ROOT
[DeviceC] dis stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    DESI  FORWARDING  ROOT
 0        GigabitEthernet1/0/2                    DESI  FORWARDING  ROOT
 0        GigabitEthernet1/0/4                    ROOT  FORWARDING  NONE
[DeviceD] dis stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/2                    ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/4                    DESI  FORWARDING  BPDU
[DeviceE] dis stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/1                    ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/4                    DESI  FORWARDING  BPDU
```

Based on the network topology, the topology for the network is shown in Figure 11.

Figure 11 Network topology



4. Verify that BPDU guard can protect edge ports from attacks:

Verify that the edge port GigabitEthernet 1/0/4 on Device D goes down when the port receives configuration BPDUs.

```
[DeviceD] display stp down-port
 Down Port                              Reason
 GigabitEthernet1/0/4                   BPDU-Protected
```

Verify that GigabitEthernet 1/0/4 goes up when it does not receive any configuration BPDUs from the peer end.

```
[DeviceD] display interface brief | include UP
InLoop0              UP   UP(s)    --
M-E0/0/0             UP   UP       192.168.2.125
NULL0                UP   UP(s)    --
GE1/0/1              UP   1G(a)   F(a)   T    1
GE1/0/2              UP   1G(a)   F(a)   T    1
GE1/0/4              UP   1G(a)   F(a)   A    1
```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
vlan 1
#
 stp instance 0 priority 4096
 stp mode rstp
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 stp root-protection
#
```

- Device B:

```
#
vlan 1
#
 stp instance 0 priority 4096
 stp mode rstp
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp root-protection
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 stp root-protection
#
```

- Device C:

```
#
vlan 1
#
 stp instance 0 priority 8192
 stp mode rstp
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 stp root-protection
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 stp root-protection
#
```

- Device D:

```
#
vlan 1
#
 stp mode rstp
 stp bpdu-protection
 stp global enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp edged-port
#
```

- Device E:

```
#
vlan 1
#
 stp mode rstp
 stp bpdu-protection
 stp global enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 stp edged-port
#
```

Contents

Introduction

This document provides examples of configuring the port-based VLAN, super VLAN, private VLAN, and voice VLAN.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of VLANs.

Example: Configuring port-based VLANs

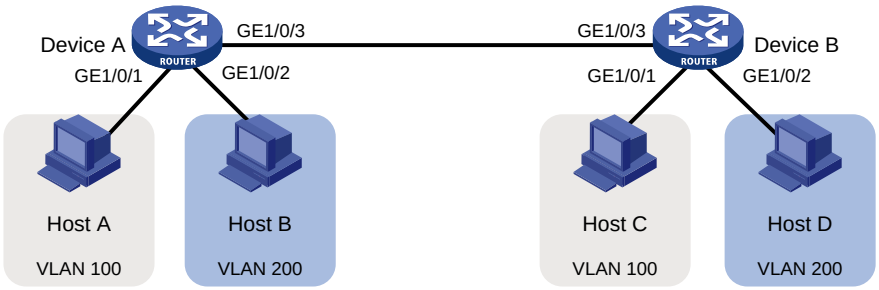
Network configuration

As shown in Figure 1:

- Host A and Host C belong to Department A. VLAN 100 is assigned to Department A.
- Host B and Host D belong to Department B. VLAN 200 is assigned to Department B.

Configure port-based VLANs so that hosts only in the same department can communicate with each other.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx

Hardware	Software version
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series	Release 63xx

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

1. Configure Device A:

Configure the ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to operate in bridge mode.

```
<DeviceA> system-view
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-mode bridge
[DeviceA-if-range] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 to VLAN 100.

```
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

Create VLAN 200, and assign GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 200
```

```
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLANs 100 and 200.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

2. Configure Device B in the same way Device A is configured. (Details not shown.)
3. Configure hosts:
   a. Configure Host A and Host C to be on the same IP subnet. For example, 192.168.100.0/24.
   b. Configure Host B and Host D to be on the same IP subnet. For example, 192.168.200.0/24.

Verifying the configuration

Verify that Host A and Host C can ping each other, but they both fail to ping Host B or Host D. (Details not shown.)

Verify that Host B and Host D can ping each other, but they both fail to ping Host A or Host C. (Details not shown.)

Display information about VLANs 100 and 200 on Device A.

```
[DeviceA-GigabitEthernet1/0/3] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/1
[DeviceA-GigabitEthernet1/0/3] display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/2
```

The output shows that:

- GigabitEthernet 1/0/3 and GigabitEthernet 1/0/1 permit packets from 100 to pass through.
- GigabitEthernet 1/0/3 and GigabitEthernet 1/0/2 permit packets from 200 to pass through.

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

Configuration files on both Device B and Device A are the same. The following configuration files use Device A as an example.

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
```

Example: Configuring the super VLAN

Network configuration

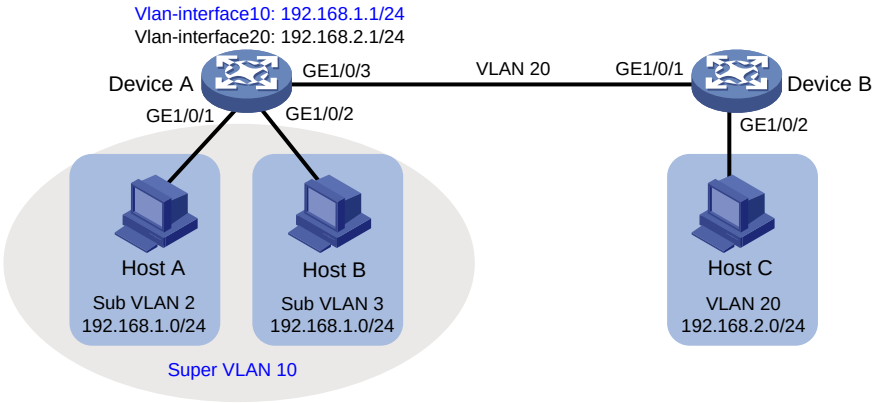
As shown in Figure 2:

- Users in VLAN 2 access the network through GigabitEthernet 1/0/1 of Device A.
- Users in VLAN 3 access the network through GigabitEthernet 1/0/2 of Device A.
- GigabitEthernet 1/0/3 of Device A and GigabitEthernet 1/0/1 of Device B are in VLAN 20.
- Users in VLAN 20 use the gateway address 192.168.2.1 and IP addresses on the IP network segment 192.168.2.0/24.

Configure a super VLAN to meet the following requirements:

- Users in VLAN 2 and VLAN 3 use the gateway address 192.168.1.1 and IP addresses on the IP network segment 192.168.1.0/24.
- Users in VLAN 2, VLAN 3, and VLAN 20 are isolated at Layer 2 but interoperable at Layer 3.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

Hardware	Software version
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Not supported

Hardware	Software version
WS5810-WiNet switch series	
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

A super VLAN does not have physical ports. A VLAN that has physical ports cannot be configured as a super VLAN.

Procedures

Configuring Device A

Create VLAN 10 and configure it as a super VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] quit
```

Create VLAN 2, and assign GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

Create VLAN 3, and assign GigabitEthernet 1/0/2 to VLAN 3.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
```

Associate super VLAN 10 with VLANs 2 and 3.

```
[DeviceA] vlan 10
[DeviceA-vlan10] subvlan 2 3
[DeviceA-vlan10] quit
```

Create VLAN-interface 10, and assign IP address 192.168.1.1 to it.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
```

Enable local proxy ARP on VLAN-interface 10.

```
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

Create VLAN 20.

```
[DeviceA] vlan 20
```

```
[DeviceA-vlan20] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and remove the port from VLAN 1.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign GigabitEthernet 1/0/3 to VLAN 20.

```
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20
```

Create VLAN-interface 20, and assign IP address 192.168.2.1 to it.

```
[DeviceA] interface Vlan-interface 20
[DeviceA-Vlan-interface20] ip address 192.168.2.1 24
[DeviceA-Vlan-interface20] quit
```

Configuring Device B

Create VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, and remove the port from VLAN 1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Assign GigabitEthernet 1/0/1 to VLAN 20.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20
```

Assign GigabitEthernet 1/0/2 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

Verifying the configuration

Verify the super VLAN configuration.

```
[DeviceA] display supervlan
 Super VLAN ID: 10
 Sub-VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 It is a super VLAN.
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports: none
 Untagged ports: none

 VLAN ID: 2
```

```
VLAN type: Static
It is a sub-VLAN.
Route interface: Configured
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0002
Name: VLAN 0002
Tagged ports: none
Untagged ports:
   GigabitEthernet1/0/1

VLAN ID: 3
VLAN type: Static
It is a sub-VLAN.
Route interface: Configured
IPv4 address: 192.168.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports: none
Untagged ports:
   GigabitEthernet1/0/2
```

Verify that Host A and Host B can ping each other. In the ARP table of Host A, the IP address of Host B corresponds to the MAC address of VLAN-interface 10. In the ARP table of Host B, the IP address of Host A corresponds to the MAC address of VLAN-interface 10. (Details not shown.)

Verify that Host A and Host C can ping each other. In the ARP table of Host A, no entry about Host C exists. In the ARP table of Host C, no entry about Host A exists. (Details not shown.)

Verify that Host B and Host C can ping each other. In the ARP table of Host B, no entry about Host C exists. In the ARP table of Host C, no entry about Host B exists. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 2
#
vlan 3
#
vlan 10
 supervlan
 subvlan 2 3
#
vlan 20
#
interface Vlan-interface10
```

```
 ip address 192.168.1.1 255.255.255.0
 local-proxy-arp enable
#
interface Vlan-interface20
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
#
```

- Device B:

```
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

Example: Configuring the private VLAN

Network configuration

As shown in Figure 3:

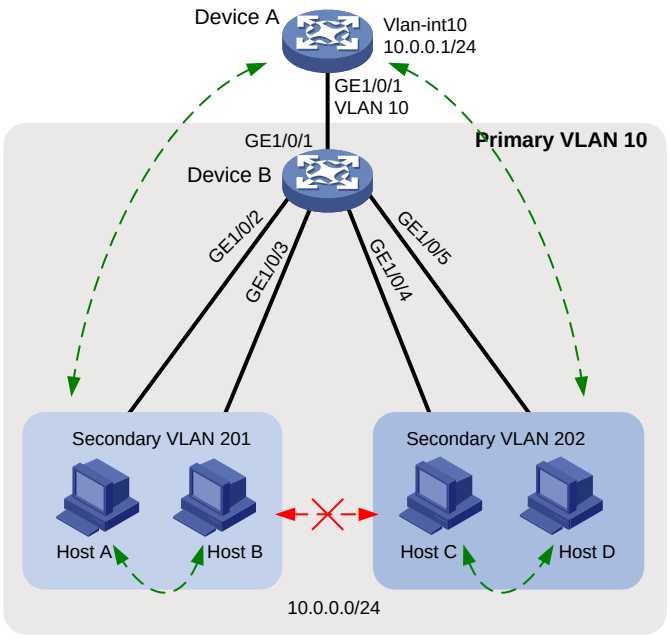
- The aggregation-layer device Device A assigns VLAN 10 to Device B. Hosts access the network through VLAN-interface 10.
- Users connected to Device B are on the same subnet 10.0.0.0/24.
- Host A and Host B are in the Marketing department. Host C and Host D are in the Finance department.

Configure the private VLAN feature to meet the following requirements:

- Device A is only aware of the primary VLAN 10.

- Hosts in the same secondary VLAN are interoperable at Layer 2.
- Hosts in different secondary VLANs are isolated at Layer 2.

Figure 3 Network diagram



Analysis

The private VLAN configuration is required only on Device B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported

Hardware	Software version
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

The system default VLAN (VLAN 1) does not support the private VLAN configuration.

Procedures

Configuring Device B

Create VLAN 10 and configure it as a primary VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

Create VLANs 201 and 202.

```
[DeviceB] vlan 201 to 202
```

Associate primary VLAN 10 with secondary VLANs 201 and 202.

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 201 to 202
[DeviceB-vlan10] quit
```

Configure the uplink port GigabitEthernet 1/0/1 as a promiscuous port of VLAN 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

Assign the downlink ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 201 as host ports.

```
[DeviceB] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[DeviceB-if-range] port link-mode bridge
[DeviceB-if-range] port access vlan 201
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
```

Assign the downlink ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5 to VLAN 202 as host ports.

```
[DeviceB] interface range gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[DeviceB-if-range] port link-mode bridge
[DeviceB-if-range] port access vlan 202
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
```

Configuring Device A

Create VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 10.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode bridge
[DeviceA-GigabitEthernet1/0/1] port access vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

Create VLAN-interface 10, and assign IP address 10.0.0.1 to it.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.0.0.1 24
[DeviceA-Vlan-interface10] quit
```

Verifying the configuration

Verify that Device A can ping Host A, Host B, Host C, and Host D successfully. (Details not shown.)

Display the ARP table of Device A.

```
[DeviceA] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI    Interface/Link ID       Aging Type
10.0.0.2        d485-64a1-7e4a 10          GE1/0/1                 19    D
10.0.0.3        7446-a0aa-7774 10          GE1/0/1                 19    D
10.0.0.4        6805-ca05-39ae 10          GE1/0/1                 20    D
10.0.0.5        6805-ca05-414e 10          GE1/0/1                 20    D
```

Display the private VLAN configuration on Device B.

```
[DeviceB] display private-vlan
 Primary VLAN ID: 10
 Secondary VLAN ID: 201-202
```

```
VLAN ID: 10
VLAN type: Static
Private VLAN type: Primary
Route interface: Not configured
Description: VLAN 0010
Name: VLAN 0010
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1          GigabitEthernet1/0/2
   GigabitEthernet1/0/3          GigabitEthernet1/0/4
   GigabitEthernet1/0/5

VLAN ID: 201
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0201
Name: VLAN 0201
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1          GigabitEthernet1/0/2
   GigabitEthernet1/0/3

VLAN ID: 202
VLAN type: Static
Private VLAN type: Secondary
Route interface: Not configured
Description: VLAN 0202
Name: VLAN 0202
Tagged ports:   None
Untagged ports:
   GigabitEthernet1/0/1          GigabitEthernet1/0/4
   GigabitEthernet1/0/5
```

The output shows that:

- The promiscuous port GigabitEthernet1/0/1 is an untagged member of primary VLAN 10 and secondary VLANs 201 and 202.
- The host ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are untagged members of secondary VLANs 201.
- The host ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5 are untagged members of secondary VLANs 202.

Verify that Hosts in the same secondary VLAN can ping each other, but they fail to ping hosts in the other secondary VLAN. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device B:

```
#
vlan 1
#
vlan 10
 private-vlan primary
 private-vlan secondary 201 to 202
#
vlan 201 to 202
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 to 202 untagged
 port hybrid pvid vlan 10
 port private-vlan 10 promiscuous
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 untagged
 port hybrid pvid vlan 201
 port private-vlan host
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 untagged
 port hybrid pvid vlan 201
 port private-vlan host
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 202 untagged
 port hybrid pvid vlan 202
 port private-vlan host
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 202 untagged
 port hybrid pvid vlan 202
```

```
 port private-vlan host
#
```

- Device A:

```
#
vlan 1
#
vlan 10
#
interface Vlan-interface10
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
```

Example: Configuring the voice VLAN

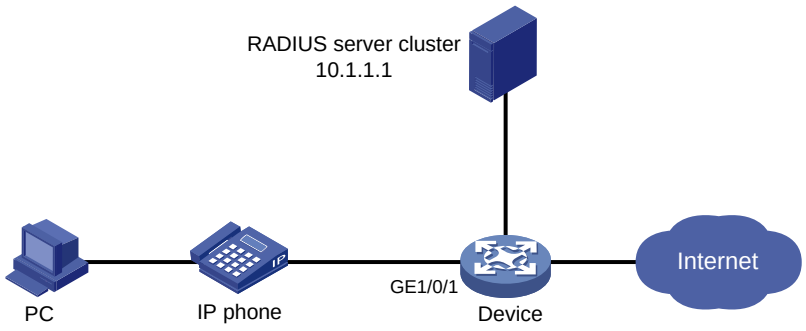
Network configuration

As shown in Figure 4, the device connects to an IP phone through GigabitEthernet1/0/1, and the IP phone sends tagged voice traffic. The device authenticates the IP phone through the RADIUS server. If the IP phone passes authentication, the IP phone is allowed to access the device. Configure voice VLAN 2 on the device. Configure LLDP to enable the IP phone to automatically come online after passing 802.1X authentication.

Configure voice VLAN to meet the following requirements:

- The IP phone automatically comes online after passing 802.1X authentication on GigabitEthernet 1/0/1.
- The IP phone can automatically come online and send voice traffic without manually configured voice VLAN MAC addresses on the device.

Figure 4 Network diagram



Analysis

- By default, an IP phone supports LLDP.
- When enabling LLDP for autodiscovering IP phones, you must configure the network-policy TLV to advertise voice VLAN information on GigabitEthernet 1/0/1.

- Enable the automatic voice VLAN assignment mode.
- Configure IP addresses for interfaces.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx

Hardware	Software version
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

Whether the username sent to the RADIUS server includes the domain name depends on the RADIUS server configuration and whether the RADIUS server accepts usernames including domain names.

- If the server does not accept usernames including domain names or the service configured for user authentication on the server does not include a domain name, specify the username not to include the domain name (**`without-domain`**) on the device.
- If the server can accept usernames including domain names and the service configured for user authentication on the server includes a domain name, specify the username to include the domain name (**`with-domain`**) on the device.

Procedures

Configuring the voice VLAN

Create VLAN 2.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] quit
```

Enable LLDP globally.

```
[Device] lldp global enable
```

Enable LLDP on GigabitEthernet 1/0/1, configure LLDP to operate in TxRx mode, and configure LLDP to advertise the voice VLAN ID.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] lldp enable
[Device-GigabitEthernet1/0/1] lldp admin-status txrx
[Device-GigabitEthernet1/0/1] lldp tlv-enable med-tlv network-policy 2
[Device-GigabitEthernet1/0/1] quit
```

Enable the voice VLAN security mode, and set the voice VLAN aging timer to 30 minutes.

```
[Device] voice-vlan security enable
[Device] voice-vlan aging 30
```

Enable LLDP for automatic IP phone discovery.

```
[Device] voice-vlan track lldp
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and configure the voice VLAN feature.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type hybrid
[Device-GigabitEthernet1/0/1] voice-vlan mode auto
[Device-GigabitEthernet1/0/1] voice-vlan 2 enable
```

Configuring 802.1X authentication

Configure the RADIUS server, add user accounts, and make sure accounting, authorization, and accounting run properly for users. (Details not shown.)

Create a RADIUS scheme. Configure the primary authentication and accounting servers and the keys for secure RADIUS authentication and accounting communication. Specify the device to remove the ISP domain name in the username sent to the RADIUS server.

```
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
[Device-radius-radius1] key authentication simple name
[Device-radius-radius1] key accounting simple money
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

Create ISP domain **bbb**, and configure 802.1X users to use RADIUS scheme **radius1** for authentication, authorization, and accounting.

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme radius1
[Device-isp-bbb] authorization lan-access radius-scheme radius1
[Device-isp-bbb] accounting lan-access radius-scheme radius1
[Device-isp-bbb] quit
```

Configure 802.1X on GigabitEthernet 1/0/1, and specify mandatory 802.1X authentication domain **bbb** on the interface.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
```

Enable the 802.1X multicast trigger feature. (Optional. By default, the 802.1X multicast trigger feature is enabled.)

```
[Device-GigabitEthernet1/0/1] dot1x multicast-trigger
[Device-GigabitEthernet1/0/1] quit
```

Enable the 802.1x feature globally.

```
[Device] dot1x
```

Configure the 802.1X client. (Details not shown.)

If you use an H3C iNode 802.1X client, for the backup authentication method local authentication to succeed, make sure the **Upload version info** option is not selected in the 802.1X connection properties.

Verifying the configuration

Display 802.1X authentication information.

```
[Device] display dot1x interface gigabitethernet 1/0/1
 Global 802.1X parameters:
   802.1X authentication               : Enabled
   CHAP authentication                 : Enabled
   Max-tx period                        : 30 s
   Handshake period                    : 15 s
   Offline detect period               : 300 s
   Quiet timer                          : Disabled
       Quiet period                     : 60 s
   Supp timeout                         : 30 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   Max auth requests                   : 2
   User aging period for Auth-Fail VLAN : 1000 s
   User aging period for Auth-Fail VSI  : 1000 s
```

```
  User aging period for critical VLAN  : 1000 s
  User aging period for critical VSI   : 1000 s
  User aging period for guest VLAN     : 1000 s
  User aging period for guest VSI      : 1000 s
  EAD assistant function               : Disabled
      EAD timeout                      : 30 min
  Domain delimiter                     : @
Online 802.1X wired users              : 1
GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Offline detection                : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : MAC-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : Not configured
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  Guest VSI                        : Not configured
  Auth-Fail VSI                    : Not configured
  Critical VSI                     : Not configured
  Add Guest VSI delay              : Disabled
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled
  Auth-Fail EAPOL                  : Disabled
  Critical EAPOL                   : Disabled
  EAPOL packets: Tx 0, Rx 0
  Sent EAP Request/Identity packets : 0
       EAP Request/Challenge packets: 0
       EAP Success packets: 0
       EAP Failure packets: 0
  Received EAPOL Start packets : 0
           EAPOL LogOff packets: 0
           EAP Response/Identity packets : 0
```

```
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 1
```

After the IP phone enters the correct username and password and then comes online, use the **display dot1x connection** command to display the connections of online users.

Display the voice VLAN state.

```
[Device] display voice-vlan state
 Current voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 30 minutes
 Voice VLAN enabled ports and their modes:
 Port                        VLAN        Mode        CoS         DSCP
 GE1/0/1                     2           Auto        6           46
```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
 voice-vlan aging 30
 voice-vlan track lldp
sable
#
 dot1x
#
 lldp global enable
#
vlan 1
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
 voice-vlan 2 enable
 lldp tlv-enable med-tlv network-policy 2
 dot1x
 dot1x mandatory-domain bbb
#
radius scheme radius1
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$/gxrbATUfK4BbF+73EQiCzBM7cwP86o=
 key accounting cipher $c$3$mq8b76RILWQr2lH7NTtvE9+7O0v7vd1H
 user-name-format without-domain
#
```

```
radius scheme system
 user-name-format without-domain
#
domain bbb
 accounting login radius-scheme radius1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
```

Contents

Introduction

This document provides examples for using VLAN tagging features to extend customer VLANs (CVLANs) across an Ethernet service provider network.

VLAN tagging features enable service providers to separate or aggregate customer traffic in the service provider network. The following are available VLAN tagging operations:

- Adding a layer of service provider VLAN (SVLAN) tag.
- Modifying the SVLAN tag, CVLAN tag, or both.

To add an SVLAN tag, use one of the following VLAN tagging features:

- **QinQ**—Tags all incoming frames (tagged or untagged) on the customer-side port with the PVID of the port.
- **One-to-two VLAN mapping**—Adds different SVLANs for traffic with different CVLAN tags.
- **Policy-based VLAN manipulation**—Uses QoS nest actions in a QoS policy to tag different classes of frames with different SVLAN tags. Traffic classifiers include CVLAN ID, IP address, and MAC address. In addition, you can use QoS priority marking to set the 802.1p priority in SVLAN tags.

To modify VLAN tags, use one of the following VLAN tagging features:

- **VLAN mapping**—Includes the following features:
  - **One-to-one VLAN mapping**—Replaces one VLAN tag with another.
  - **Two-to-two VLAN mapping**—Replaces the SVLAN ID, CVLAN ID, or both IDs for an incoming double-tagged frame.
- **Policy-based VLAN manipulation**—Uses a QoS policy to modify the CVLAN or SVLAN ID by using the **remark customer-vlan-id** or **remark service-vlan-id** action.

The devices in the service provider network learn MAC addresses of CVLANs into the MAC address table of the SVLAN.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of QinQ, VLAN mapping, QoS nesting, and QoS priority and CVLAN marking.

Example: Configuring QinQ

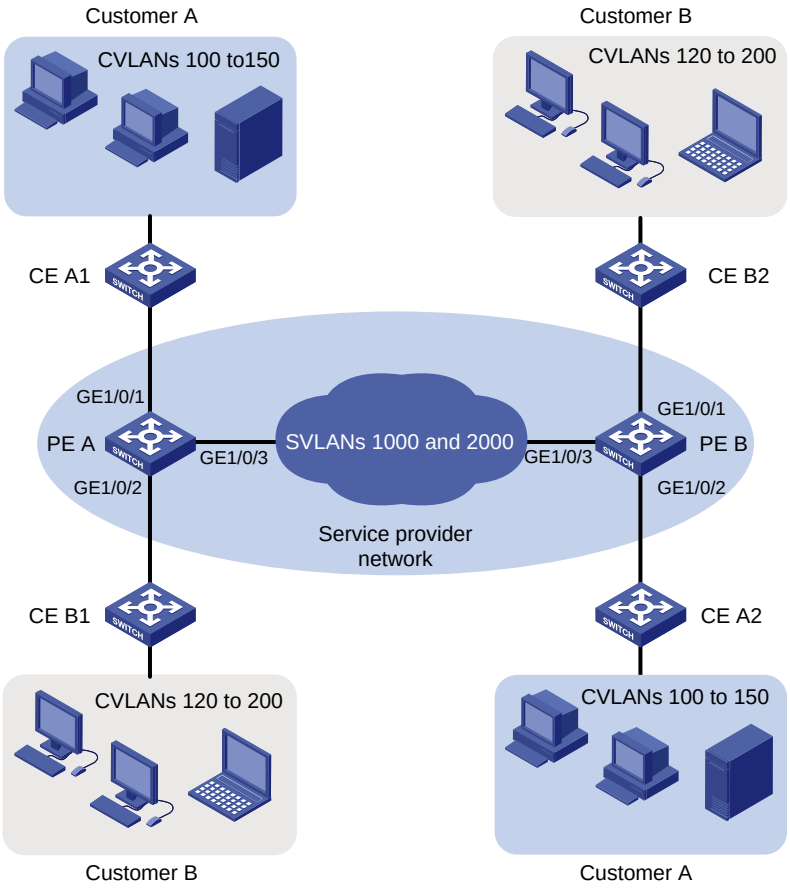
Network configuration

As shown in Figure 1:

- The service provider assigns VLAN 1000 to Company A's VLANs 100 through 150.
- The service provider assigns VLAN 2000 to Company B's VLANs 120 through 200.

Configure QinQ on PE A and PE B to transmit traffic in VLANs 1000 and 2000 for Company A and Company B, respectively.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series	Not supported

Hardware	Software version
S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure QinQ, follow these restrictions and guidelines:

- You only need to configure QinQ on customer-side ports of PEs.
- The link type of the customer-side port can be access, hybrid, or trunk.
  - If the link type is access, you must assign the port to the SVLAN.
  - If the link type is trunk, you must assign the port to the SVLAN, and set the SVLAN ID as the PVID of the port.
  - If the link type is hybrid, you must assign the port to the SVLAN as an untagged VLAN member, and set the SVLAN ID as the PVID of the port. The settings ensure that the port can forward traffic to the customer site with the SVLAN tag removed.
- For QinQ frames to travel across the service provider network, you must perform the following tasks:
  - Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. This value is the sum of the default Ethernet interface MTU (1500 bytes) and the length (4 bytes) of a CVLAN tag. The CVLAN tag of QinQ frames is treated as part of the payload during transmission.
  - Configure all the ports on the forwarding path to allow frames from VLANs 1000 and 2000 to pass through without removing the VLAN tag.

Procedures

Configuring PE A

1. Create VLANs 1000 and 2000.

```
<PE_A> system-view
[PE_A] vlan 1000
[PE_A-vlan1000] quit
[PE_A] vlan 2000
[PE_A-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1:

   # Configure the port as an access port, and assign the port to VLAN 1000.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port access vlan 1000
```

   # Enable QinQ on the port.

```
[PE_A-GigabitEthernet1/0/1] qinq enable
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

   # Configure the port as an access port, and assign the port to VLAN 2000.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port access vlan 2000
```

   # Enable QinQ on the port.

```
[PE_A-GigabitEthernet1/0/2] qinq enable
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

   # Configure the port as a trunk port.

```
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
```

   # Assign the port to VLANs 1000 and 2000.

```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

   # Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE_A-GigabitEthernet1/0/3] quit
```

Configuring PE B

1. Create VLANs 1000 and 2000.

```
<PE_B> system-view
[PE_B] vlan 1000
[PE_B-vlan1000] quit
[PE_B] vlan 2000
[PE_B-vlan2000] quit
```

2. Configure GigabitEthernet 1/0/1:

   # Configure the port as an access port, and assign the port to VLAN 2000.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port access vlan 2000
```

Enable QinQ on the port.

```
[PE_B-GigabitEthernet1/0/1] qinq enable
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

   # Configure the port as an access port, and assign the port to VLAN 1000.

   ```
   [PE_B] interface gigabitethernet 1/0/2
   [PE_B-GigabitEthernet1/0/2] port access vlan 1000
   ```

   # Enable QinQ on the port.

   ```
   [PE_B-GigabitEthernet1/0/2] qinq enable
   [PE_B-GigabitEthernet1/0/2] quit
   ```

4. Configure GigabitEthernet 1/0/3:

   # Configure the port as a trunk port.

   ```
   [PE_B] interface gigabitethernet 1/0/3
   [PE_B-GigabitEthernet1/0/3] port link-type trunk
   ```

   # Assign the port to VLANs 1000 and 2000.

   ```
   [PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
   ```

   # Remove the port from VLAN 1.

   ```
   [PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
   [PE_B-GigabitEthernet1/0/3] quit
   ```

Configuring devices between PE A and PE B

Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)

Configure all ports on the forwarding path to allow frames from VLANs 1000 and 2000 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Verify that each company's PCs can ping each other in the same CVLAN across the service provider network. (Details not shown.)

Verify that the two companies' PCs cannot communicate at Layer 2 even if their CVLAN IDs are the same. The ARP tables on one company's PCs do not contain entries for MAC addresses of the other company's PCs. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- PE A:

  ```
  #
  vlan 1000
  #
  vlan 2000
  #
  interface GigabitEthernet1/0/1
  ```

```
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#
```

- PE B:

```
#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2000
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000 2000
#
#
```

Example: Configuring one-to-two VLAN mapping

Network configuration

As shown in Figure 2:

- Customer A and Customer B each have two branches that require Layer 2 connectivity over the service provider network.
- Both customers have three types of traffic. For each customer, the service provider assigns one SVLAN by traffic type.

Configure one-to-two VLAN mapping on each customer-side port of PE A and PE B to meet the following requirements:

- The service provider adds an SVLAN tag to packets from customer networks based on the traffic type, as described in Table 1 and Figure 3.
- The SVLAN tag uses the same 802.1p priority as the CVLAN tag.

Figure 2 Network diagram

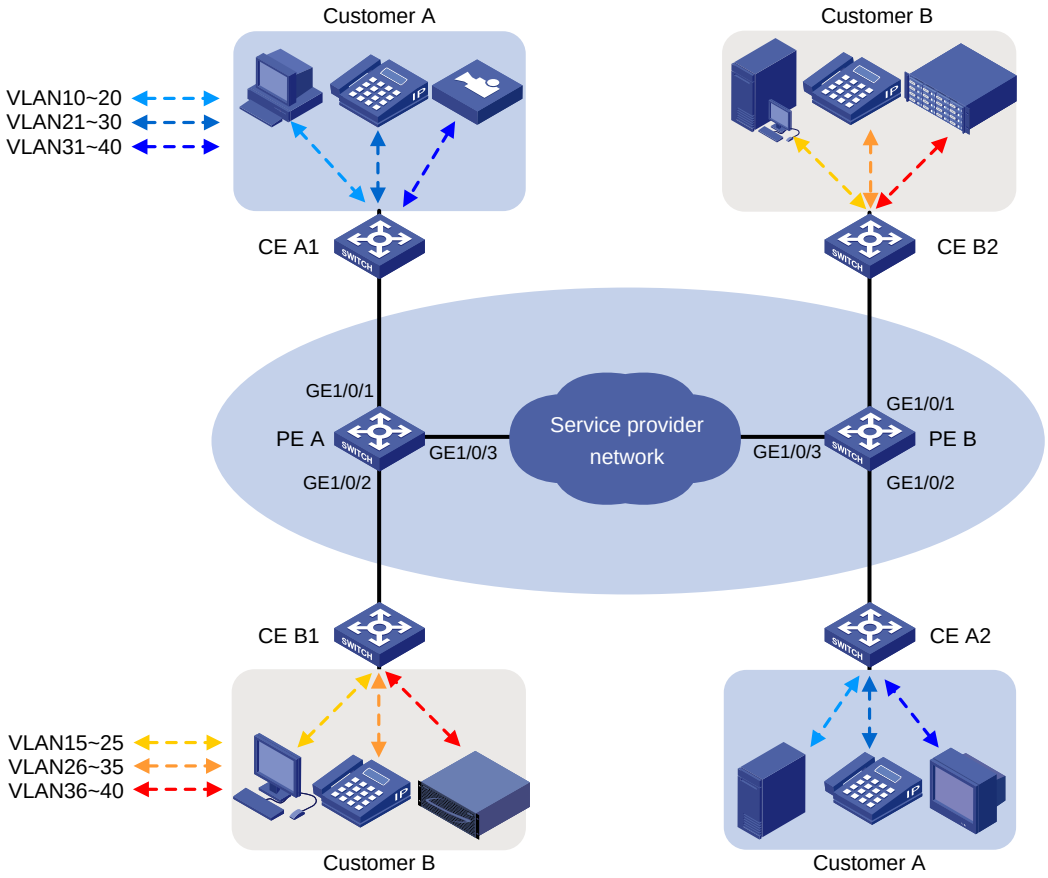
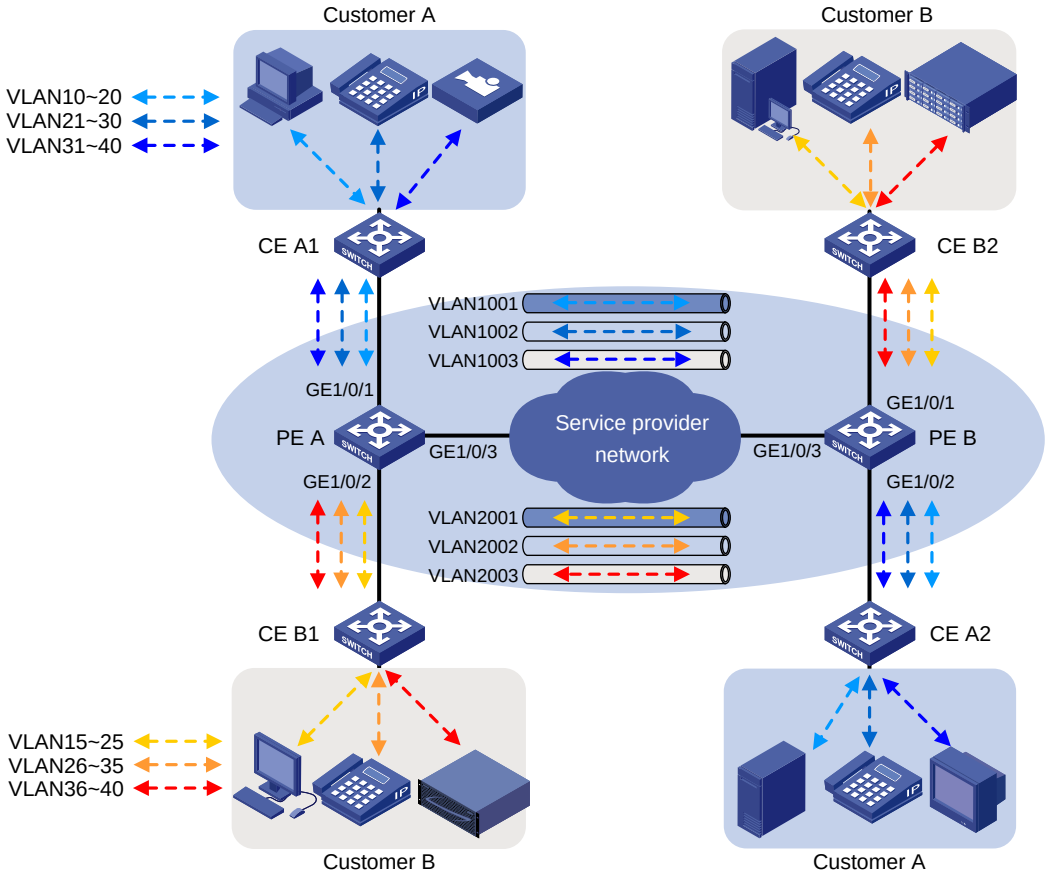


Table 1 VLAN mapping table

Traffic type	CVLANs	SVLAN
Customer A		
Video	31 to 40	1003
Voice	21 to 30	1002
Data	10 to 20	1001
Customer B		
Storage	36 to 40	2003
Voice	26 to 35	2002

Traffic type	CVLANs	SVLAN
Data	15 to 25	2001

Figure 3 Required traffic pattern in the service provider network



Analysis

To support multiple SVLANs and send traffic to the customer networks with the SVLAN tag removed, perform the following tasks on the customer-side ports:

1. Configure the link type of the ports as hybrid.
2. Assign the ports to the SVLANs as untagged VLAN members.

For the SVLAN tag to use the same 802.1p priority as the CVLAN tag, configure the customer-side port to use the 802.1p priority in incoming packets for priority mapping.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series	Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6813 switch series	
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and	Release 63xx

Hardware	Software version
S5120V3-54P-PWR-SI)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure ports on the forwarding path of double-tagged packets across the service provider network, follow these restrictions and guidelines:

- Set the MTU to a minimum of 1504 bytes for each port.
- Configure all ports to allow double-tagged packets to pass through without removing the SVLAN tag.

Procedures

Configuring PE A

1. Create CVLANs and SVLANs:

   # Create CVLANs 10 to 40.

   ```
   <PE_A> system-view
   [PE_A] vlan 10 to 40
   ```

   # Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

   ```
   [PE_A] vlan 1001 to 1003
   [PE_A] vlan 2001 to 2003
   ```

2. Configure the customer-side port GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port.

   ```
   [PE_A] interface gigabitethernet 1/0/1
   [PE_A-GigabitEthernet1/0/1] port link-type hybrid
   ```

   # Assign the port to CVLANs 10 through 40 as a tagged VLAN member.

   ```
   [PE_A-GigabitEthernet1/0/1] port hybrid vlan 10 to 40 tagged
   ```

   # Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

   ```
   [PE_A-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
   ```

   # Remove the port from VLAN 1.

   ```
   [PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
   ```

   # Configure one-to-two VLAN mapping to add SVLAN tag 1001 to traffic from VLANs 10 through 20.

   ```
   [PE_A-GigabitEthernet1/0/1] vlan mapping nest range 10 to 20 nested-vlan 1001
   ```

   # Configure one-to-two VLAN mapping to add SVLAN tag 1002 to traffic from VLANs 21 through 30.

   ```
   [PE_A-GigabitEthernet1/0/1] vlan mapping nest range 21 to 30 nested-vlan 1002
   ```

   # Configure one-to-two VLAN mapping to add SVLAN tag 1003 to traffic from VLANs 31 through 40.

   ```
   [PE_A-GigabitEthernet1/0/1] vlan mapping nest range 31 to 40 nested-vlan 1003
   ```

   # Configure the port to use the 802.1p priority in incoming packets for priority mapping.

   ```
   [PE_A-GigabitEthernet1/0/1] qos trust dot1p
   [PE_A-GigabitEthernet1/0/1] quit
   ```

3. Configure the customer-side port GigabitEthernet 1/0/2:

   # Configure the port as a hybrid port.

   ```
   [PE_A] interface gigabitethernet 1/0/2
   [PE_A-GigabitEthernet1/0/2] port link-type hybrid
   ```

   # Assign the port to CVLANs 15 through 40 as a tagged VLAN member.

   ```
   [PE_A-GigabitEthernet1/0/2] port hybrid vlan 15 to 40 tagged
   ```

   # Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

   ```
   [PE_A-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
   ```

   # Remove the port from VLAN 1.

   ```
   [PE_A-GigabitEthernet1/0/2] undo port hybrid vlan 1
   ```

   # Configure one-to-two VLAN mapping to add SVLAN tag 2001 to traffic from VLANs 15 through 25.

   ```
   [PE_A-GigabitEthernet1/0/2] vlan mapping nest range 15 to 25 nested-vlan 2001
   ```

Configure one-to-two VLAN mapping to add SVLAN tag 2002 to traffic from VLANs 26 through 35.

```
[PE_A-GigabitEthernet1/0/2] vlan mapping nest range 26 to 35 nested-vlan 2002
```

Configure one-to-two VLAN mapping to add SVLAN tag 2003 to traffic from VLANs 36 through 40.

```
[PE_A-GigabitEthernet1/0/2] vlan mapping nest range 36 to 40 nested-vlan 2003
```

Configure the port to use the 802.1p priority in incoming packets for priority mapping.

```
[PE_A-GigabitEthernet1/0/2] qos trust dot1p
[PE_A-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port GigabitEthernet 1/0/3:

Configure the port as a trunk port.

```
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
```

Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-GigabitEthernet1/0/3] quit
```

Configuring PE B

1. Create CVLANs and SVLANs:

Create CVLANs 10 to 40.

```
<PE_B> system-view
[PE_B] vlan 10 to 40
```

Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B] vlan 1001 to 1003
[PE_B] vlan 2001 to 2003
```

2. Configure the customer-side port GigabitEthernet 1/0/1:

Configure the port as a hybrid port.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
```

Assign the port to CVLANs 15 through 40 as a tagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 15 to 40 tagged
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Configure one-to-two VLAN mapping to add SVLAN tag 2001 to traffic from VLANs 15 through 25.

```
[PE_B-GigabitEthernet1/0/1] vlan mapping nest range 15 to 25 nested-vlan 2001
```

Configure one-to-two VLAN mapping to add SVLAN tag 2002 to traffic from VLANs 26 through 35.

```
[PE_B-GigabitEthernet1/0/1] vlan mapping nest range 26 to 35 nested-vlan 2002
```

Configure one-to-two VLAN mapping to add SVLAN tag 2003 to traffic from VLANs 36 through 40.

```
[PE_B-GigabitEthernet1/0/1] vlan mapping nest range 36 to 40 nested-vlan 2003
```

Configure the port to use the 802.1p priority in incoming packets for priority mapping.

```
[PE_B-GigabitEthernet1/0/1] qos trust dot1p
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port GigabitEthernet 1/0/2:

Configure the port as a hybrid port.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type hybrid
```

Assign the port to CVLANs 10 through 40 as a tagged VLAN member.

```
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 10 to 40 tagged
```

Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Configure one-to-two VLAN mapping to add SVLAN tag 1001 to traffic from VLANs 10 through 20.

```
[PE_B-GigabitEthernet1/0/2] vlan mapping nest range 10 to 20 nested-vlan 1001
```

Configure one-to-two VLAN mapping to add SVLAN tag 1002 to traffic from VLANs 21 through 30.

```
[PE_B-GigabitEthernet1/0/2] vlan mapping nest range 21 to 30 nested-vlan 1002
```

Configure one-to-two VLAN mapping to add SVLAN tag 1003 to traffic from VLANs 31 through 40.

```
[PE_B-GigabitEthernet1/0/2] vlan mapping nest range 31 to 40 nested-vlan 1003
```

Configure the port to use the 802.1p priority in incoming packets for priority mapping.

```
[PE_B-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port GigabitEthernet 1/0/3:

Configure the port as a trunk port.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-GigabitEthernet1/0/3] quit
```

Configuring devices between PE A and PE B

Set the MTU to a minimum of 1504 bytes for each port on the path of double-tagged packets. (Details not shown.)

Configure all ports on the forwarding path to allow packets from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the SVLAN tag. (Details not shown.)

Verifying the configuration

1. Verify VLAN mapping information:

Verify VLAN mapping information on PE A.

```
[PE_A] display vlan mapping
Interface GigabitEthernet1/0/1:
```

```
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10-20         N/A           1001                     10-20
  21-30         N/A           1002                     21-30
  31-40         N/A           1003                     31-40
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  15-25         N/A           2001                     15-25
  26-35         N/A           2002                     26-35
  36-40         N/A           2003                     36-40
```

Verify VLAN mapping information on PE B.

```
[PE_B] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  15-25         N/A           2001                     15-25
  26-35         N/A           2002                     26-35
  36-40         N/A           2003                     36-40
Interface GigabitEthernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  10-20         N/A           1001                     10-20
  21-30         N/A           1002                     21-30
  31-40         N/A           1003                     31-40
```

2. Verify that PCs of the same customer in a CVLAN can ping each other across the service provider network. (Details not shown.)
3. Verify that PCs of different customers in a CVLAN cannot communicate at Layer 2. The ARP tables on one customer's PCs do not contain entries for MAC addresses of the other customer's PCs. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- PE A:

```
#
vlan 10 to 40
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 to 40 tagged
 port hybrid vlan 1001 to 1003 untagged
 vlan mapping nest range 10 to 20 nested-vlan 1001
 vlan mapping nest range 21 to 30 nested-vlan 1002
 vlan mapping nest range 31 to 40 nested-vlan 1003
```

```
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 15 to 40 tagged
 port hybrid vlan 2001 to 2003 untagged
 vlan mapping nest range 15 to 25 nested-vlan 2001
 vlan mapping nest range 26 to 35 nested-vlan 2002
 vlan mapping nest range 36 to 40 nested-vlan 2003
 qos trust dot1p
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

- PE B:

```
#
vlan 10 to 40
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 15 to 40 tagged
 port hybrid vlan 2001 to 2003 untagged
 vlan mapping nest range 15 to 25 nested-vlan 2001
 vlan mapping nest range 26 to 35 nested-vlan 2002
 vlan mapping nest range 36 to 40 nested-vlan 2003
 qos trust dot1p
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 to 40 tagged
 port hybrid vlan 1001 to 1003 untagged
 vlan mapping nest range 10 to 20 nested-vlan 1001
 vlan mapping nest range 21 to 30 nested-vlan 1002
 vlan mapping nest range 31 to 40 nested-vlan 1003
 qos trust dot1p
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

Example: Configuring QoS policies for SVLAN tagging and 802.1p priority marking

Network configuration

As shown in Figure 4:

- Customer A and Customer B each have two branches that require Layer 2 connectivity over the service provider network.
- Both customers have three types of traffic and require different transmission priorities for the three types of traffic.

Apply a QoS policy to each customer-side port on PE A and PE B to meet the following requirements:

- Separate the traffic by customer and traffic type.
- Assign different 802.1p priority values to the traffic flows.

Figure 4 Network diagram

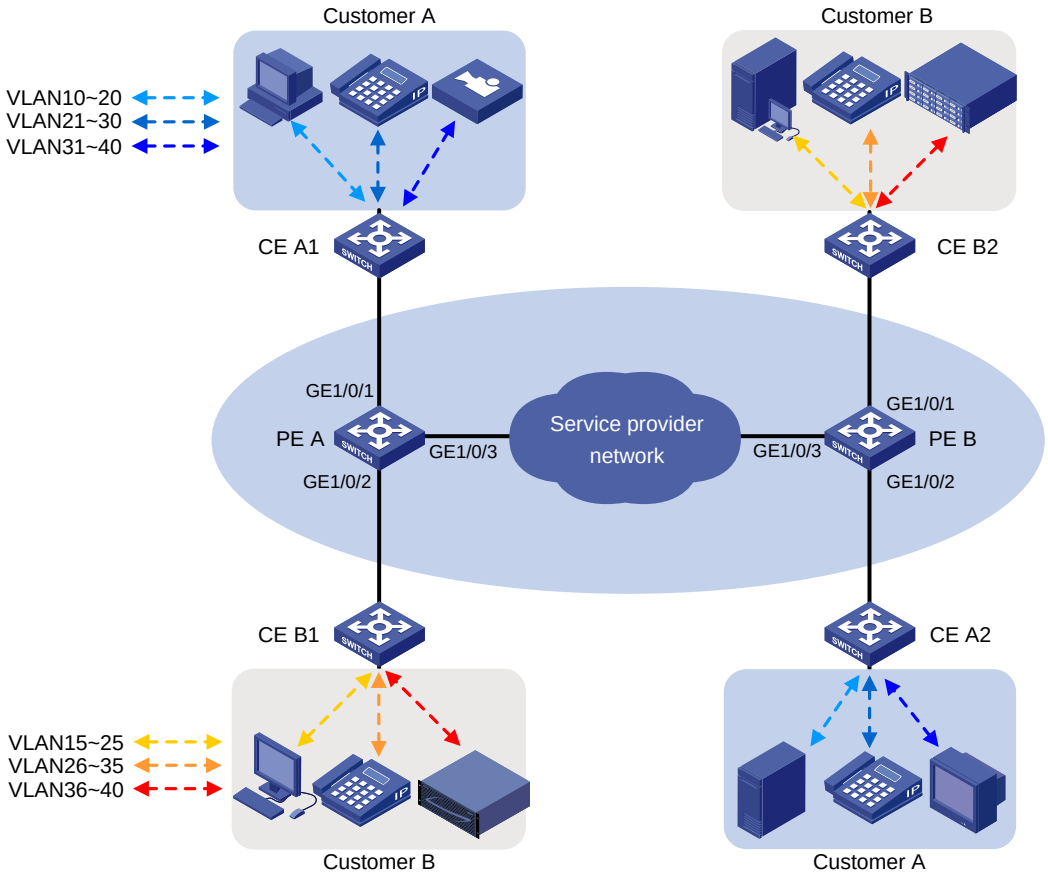
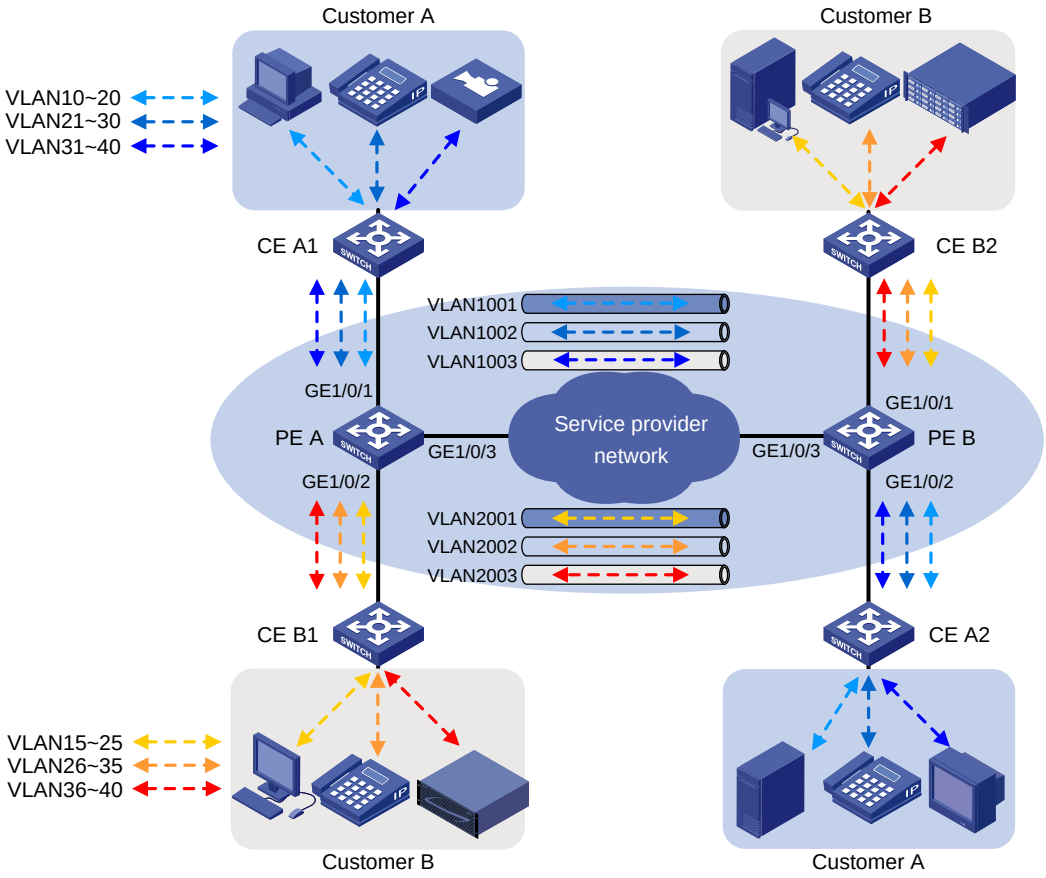


Table 2 shows the VLAN and 802.1p priority assignment scheme. For each customer, the service provider assigns one SVLAN by traffic type. Figure 5 shows the expected traffic transmission pattern after the QoS policies are applied to customer-side ports.

Table 2 VLAN and traffic priority assignment

Traffic type	CVLANs	SVLAN	Traffic priority
Customer A:			
Video	31 to 40	1003	High
Voice	21 to 30	1002	Medium
Data	10 to 20	1001	Low
Customer B:			
Storage	36 to 40	2003	High
Voice	26 to 35	2002	Medium
Data	15 to 25	2001	Low

Figure 5 Expected traffic pattern in the service provider network



Analysis

For the customer-side ports to support multiple SVLANs and send traffic to the customer site with the SVLAN tag removed, you must perform the following tasks:

1. Configure the link type as hybrid on the customer-side ports.
2. Assign the ports to the SVLANs as untagged VLAN members.

To change the 802.1p priority for a class of traffic, use the **remark dot1p** action. By default, the 802.1p priority in the SVLAN tag added by a QinQ-enabled port depends on the priority trust mode on the port.

- If the 802.1p priority in frames is trusted, the device copies the 802.1p priority in the CVLAN tag to the SVLAN tag.
- If port priority is trusted, the port priority is used as the 802.1p priority in the SVLAN tag. For untagged incoming frames, the port encapsulates the port priority as the 802.1p priority in the SVLAN tag.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except	Release 11xx

Hardware	Software version
S5500V3-24P-SI and S5500V3-48P-SI)	
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4520 switch series	Release 66xx

Hardware	Software version
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an SVLAN tagging QoS policy, follow these restrictions and guidelines:

- Use the nest action for SVLAN tagging. You can configure only one nest action in the traffic behavior for a traffic class.
- You must apply the QoS policy to the inbound direction of customer-side ports.
- If an incoming frame does not match the QoS policy, the port adds the PVID tag to the frame as the SVLAN tag.

For QinQ frames to travel across the service provider network, follow these restrictions and guidelines:

- Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. This value is the sum of the default Ethernet interface MTU (1500 bytes) and the length (4 bytes) of a CVLAN tag. The CVLAN tag of QinQ frames is treated as part of the payload during transmission.
- Configure all the ports on the forwarding path to allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the VLAN tag.

Procedures

Configuring PE A

1. Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
<PE_A> system-view
[PE_A] vlan 1001 to 1003
[PE_A] vlan 2001 to 2003
```

2. Configure the customer-side port GigabitEthernet 1/0/1:

   # Configure the port as a hybrid port.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
```

   # Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

   # Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 1001 to 1003 untagged
```

   # Enable QinQ on the port.

```
[PE_A-GigabitEthernet1/0/1] qinq enable
```

   # Configure the port to trust the 802.1p priority of frames.

```
[PE_A-GigabitEthernet1/0/1] qos trust dot1p
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port GigabitEthernet 1/0/2:

   # Configure the port as a hybrid port.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port link-type hybrid
```

   # Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_A-GigabitEthernet1/0/2] port hybrid vlan 2001 to 2003 untagged
```

Enable QinQ on the port.

```
[PE_A-GigabitEthernet1/0/2] qinq enable
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_A-GigabitEthernet1/0/2] qos trust dot1p
[PE_A-GigabitEthernet1/0/2] quit
```

3. Configure the service provider-side port GigabitEthernet 1/0/3:

Configure the port as a trunk port.

```
[PE_A] interface gigabitethernet 1/0/3
[PE_A-GigabitEthernet1/0/3] port link-type trunk
```

Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_A-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_A-GigabitEthernet1/0/3] quit
```

4. Configure QoS policies for SVLAN tagging and 802.1p priority marking:

Create the class **customer_A_pc** to match traffic from CVLANs 10 through 20 (data traffic) for Customer A.

```
[PE_A] traffic classifier customer_A_pc
[PE_A-classifier-customer_A_pc] if-match customer-vlan-id 10 to 20
[PE_A-classifier-customer_A_pc] quit
```

Create the classes **customer_A_voice** and **customer_A_video** to match Customer A's voice traffic and video traffic, respectively.

```
[PE_A] traffic classifier customer_A_voice
[PE_A-classifier-customer_A_voice] if-match customer-vlan-id 21 to 30
[PE_A-classifier-customer_A_voice] quit
[PE_A] traffic classifier customer_A_video
[PE_A-classifier-customer_A_video] if-match customer-vlan-id 31 to 40
[PE_A-classifier-customer_A_video] quit
```

Configure SVLAN tagging and 802.1p priority marking actions for Customer A's three traffic types.

```
[PE_A] traffic behavior customer_A_pc
[PE_A-behavior-customer_A_pc] nest top-most vlan 1001
[PE_A-behavior-customer_A_pc] remark dot1p 3
[PE_A-behavior-customer_A_pc] quit
[PE_A] traffic behavior customer_A_voice
[PE_A-behavior-customer_A_voice] nest top-most vlan 1002
[PE_A-behavior-customer_A_voice] remark dot1p 5
[PE_A-behavior-customer_A_voice] quit
[PE_A] traffic behavior customer_A_video
[PE_A-behavior-customer_A_video] nest top-most vlan 1003
[PE_A-behavior-customer_A_video] remark dot1p 7
[PE_A-behavior-customer_A_video] quit
```

Create the QoS policy **customer_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_A
```

```
[PE_A-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_A-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_A-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_A-qospolicy-customer_A] quit
```

Apply the QoS policy **customer_A** to the inbound direction of GigabitEthernet 1/0/1.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] qos apply policy customer_A inbound
[PE_A-GigabitEthernet1/0/1] quit
```

Create traffic classes for matching Customer B's three traffic types.

```
[PE_A] traffic classifier customer_B_pc
[PE_A-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_A-classifier-customer_B_pc] quit
[PE_A] traffic classifier customer_B_voice
[PE_A-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_A-classifier-customer_B_voice] quit
[PE_A] traffic classifier customer_B_storage
[PE_A-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_A-classifier-customer_B_storage] quit
```

Configure SVLAN tagging and 802.1p priority marking behaviors for Customer B's traffic types.

```
[PE_A] traffic behavior customer_B_pc
[PE_A-behavior-customer_B_pc] nest top-most vlan 2001
[PE_A-behavior-customer_B_pc] remark dot1p 3
[PE_A-behavior-customer_B_pc] quit
[PE_A] traffic behavior customer_B_voice
[PE_A-behavior-customer_B_voice] nest top-most vlan 2002
[PE_A-behavior-customer_B_voice] remark dot1p 5
[PE_A-behavior-customer_B_voice] quit
[PE_A] traffic behavior customer_B_storage
[PE_A-behavior-customer_B_storage] nest top-most vlan 2003
[PE_A-behavior-customer_B_storage] remark dot1p 7
[PE_A-behavior-customer_B_storage] quit
```

Create the QoS policy **customer_B** for Customer B, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_A] qos policy customer_B
[PE_A-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_A-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_A-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_A-qospolicy-customer_B] quit
```

Apply the QoS policy **customer_B** to the inbound direction of GigabitEthernet 1/0/2.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] qos apply policy customer_B inbound
[PE_A-GigabitEthernet1/0/2] quit
```

Configuring PE B

1. Create SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
<PE_B> system-view
[PE_B] vlan 1001 to 1003
[PE_B] vlan 2001 to 2003
```

2. Configure the customer-side port GigabitEthernet 1/0/1:

Configure the port as a hybrid port.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
```

Assign the port to SVLANs 2001 through 2003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 2001 to 2003 untagged
```

Enable QinQ on the port.

```
[PE_B-GigabitEthernet1/0/1] qinq enable
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-GigabitEthernet1/0/1] qos trust dot1p
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure the customer-side port GigabitEthernet 1/0/2:

Configure the port as a hybrid port.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type hybrid
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/2] undo port hybrid vlan 1
```

Assign the port to SVLANs 1001 through 1003 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/2] port hybrid vlan 1001 to 1003 untagged
```

Enable QinQ on the port.

```
[PE_B-GigabitEthernet1/0/2] qinq enable
```

Configure the port to trust the 802.1p priority of frames.

```
[PE_B-GigabitEthernet1/0/2] qos trust dot1p
[PE_B-GigabitEthernet1/0/2] quit
```

4. Configure the service provider-side port GigabitEthernet 1/0/3:

Configure the port as a trunk port.

```
[PE_B] interface gigabitethernet 1/0/3
[PE_B-GigabitEthernet1/0/3] port link-type trunk
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Assign the port to SVLANs 1001 through 1003 and SVLANs 2001 through 2003.

```
[PE_B-GigabitEthernet1/0/3] port trunk permit vlan 1001 to 1003 2001 to 2003
[PE_B-GigabitEthernet1/0/3] quit
```

5. Configure QoS policies for SVLAN tagging and 802.1p priority marking:

Create traffic classes for matching Customer A's traffic types.

```
[PE_B] traffic classifier customer_A_pc
[PE_B-classifier-customer_A_pc] if-match customer-vlan-id 10 to 20
[PE_B-classifier-customer_A_pc] quit
[PE_B] traffic classifier customer_A_voice
[PE_B-classifier-customer_A_voice] if-match customer-vlan-id 21 to 30
[PE_B-classifier-customer_A_voice] quit
[PE_B] traffic classifier customer_A_video
```

```
[PE_B-classifier-customer_A_video] if-match customer-vlan-id 31 to 40
[PE_B-classifier-customer_A_video] quit
```

Configure SVLAN tagging and 802.1p priority marking behaviors for Customer A's three traffic types.

```
[PE_B] traffic behavior customer_A_pc
[PE_B-behavior-customer_A_pc] nest top-most vlan 1001
[PE_B-behavior-customer_A_pc] remark dot1p 3
[PE_B-behavior-customer_A_pc] quit
[PE_B] traffic behavior customer_A_voice
[PE_B-behavior-customer_A_voice] nest top-most vlan 1002
[PE_B-behavior-customer_A_voice] remark dot1p 5
[PE_B-behavior-customer_A_voice] quit
[PE_B] traffic behavior customer_A_video
[PE_B-behavior-customer_A_video] nest top-most vlan 1003
[PE_B-behavior-customer_A_video] remark dot1p 7
[PE_B-behavior-customer_A_video] quit
```

Create the QoS policy **customer_A** for Customer A, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_B] qos policy customer_A
[PE_B-qospolicy-customer_A] classifier customer_A_pc behavior customer_A_pc
[PE_B-qospolicy-customer_A] classifier customer_A_voice behavior customer_A_voice
[PE_B-qospolicy-customer_A] classifier customer_A_video behavior customer_A_video
[PE_B-qospolicy-customer_A] quit
```

Apply the QoS policy **customer_A** to the inbound direction of GigabitEthernet 1/0/2.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] qos apply policy customer_A inbound
[PE_B-GigabitEthernet1/0/2] quit
```

Create traffic classes for matching Customer B's three traffic types.

```
[PE_B] traffic classifier customer_B_pc
[PE_B-classifier-customer_B_pc] if-match customer-vlan-id 15 to 25
[PE_B-classifier-customer_B_pc] quit
[PE_B] traffic classifier customer_B_voice
[PE_B-classifier-customer_B_voice] if-match customer-vlan-id 26 to 35
[PE_B-classifier-customer_B_voice] quit
[PE_B] traffic classifier customer_B_storage
[PE_B-classifier-customer_B_storage] if-match customer-vlan-id 36 to 40
[PE_B-classifier-customer_B_storage] quit
```

Configure SVLAN tagging and 802.1p priority marking behaviors for Customer B's three traffic types.

```
[PE_B] traffic behavior customer_B_pc
[PE_B-behavior-customer_B_pc] nest top-most vlan 2001
[PE_B-behavior-customer_B_pc] remark dot1p 3
[PE_B-behavior-customer_B_pc] quit
[PE_B] traffic behavior customer_B_voice
[PE_B-behavior-customer_B_voice] nest top-most vlan 2002
[PE_B-behavior-customer_B_voice] remark dot1p 5
[PE_B-behavior-customer_B_voice] quit
[PE_B] traffic behavior customer_B_storage
```

```
[PE_B-behavior-customer_B_storage] nest top-most vlan 2003
[PE_B-behavior-customer_B_storage] remark dot1p 7
[PE_B-behavior-customer_B_storage] quit
```

Create the QoS policy **customer_B** for Customer B, and associate the classes with their respective behaviors in the QoS policy.

```
[PE_B] qos policy customer_B
[PE_B-qospolicy-customer_B] classifier customer_B_pc behavior customer_B_pc
[PE_B-qospolicy-customer_B] classifier customer_B_voice behavior customer_B_voice
[PE_B-qospolicy-customer_B] classifier customer_B_storage behavior
customer_B_storage
[PE_B-qospolicy-customer_B] quit
```

Apply the QoS policy **customer_B** to the inbound direction of GigabitEthernet 1/0/1.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] qos apply policy customer_B inbound
[PE_B-GigabitEthernet1/0/1] quit
```

Configuring devices between PE A and PE B

Set the MTU to a minimum of 1504 bytes for each port on the path of QinQ frames. (Details not shown.)

Configure all ports on the path between PE A and PE B allow frames from VLANs 1001 through 1003 and VLANs 2001 through 2003 to pass through without removing the VLAN tag. (Details not shown.)

Verifying the configuration

Verify the configuration on each port. This example uses GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
Return
[PE_A-GigabitEthernet1/0/1] quit
```

Verify the QoS configuration on each port. This example uses GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: customer_A
```

```
Classifier: customer_A_pc
  Operator: AND
  Rule(s) :
   If-match customer-vlan-id 10 to 20
  Behavior: customer_A_pc
   Nesting:
     Nest top-most vlan-id 1001
   Marking:
     Remark dot1p 3
Classifier: customer_A_voice
  Operator: AND
  Rule(s) :
   If-match customer-vlan-id 21 to 30
  Behavior: customer_A_voice
   Nesting:
     Nest top-most vlan-id 1002
   Marking:
     Remark dot1p 5
Classifier: customer_A_video
  Operator: AND
  Rule(s) :
   If-match customer-vlan-id 31 to 40
  Behavior: customer_A_video
   Nesting:
     Nest top-most vlan-id 1003
   Marking:
     Remark dot1p 7
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- PE A:

```
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
#
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
#
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
#
```

```
traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
#
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
#
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 nest top-most vlan 1001
 remark dot1p 3
#
traffic behavior customer_A_voice
 nest top-most vlan 1002
 remark dot1p 5
#
traffic behavior customer_A_video
 nest top-most vlan 1003
 remark dot1p 7
#
traffic behavior customer_B_pc
 nest top-most vlan 2001
 remark dot1p 3
#
traffic behavior customer_B_voice
 nest top-most vlan 2002
 remark dot1p 5
#
traffic behavior customer_B_storage
 nest top-most vlan 2003
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
#
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
```

```
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

- PE B:

```
#
vlan 1001 to 1003
#
vlan 2001 to 2003
#
traffic classifier customer_A_pc operator and
 if-match customer-vlan-id 10 to 20
#
traffic classifier customer_A_voice operator and
 if-match customer-vlan-id 21 to 30
#
traffic classifier customer_A_video operator and
 if-match customer-vlan-id 31 to 40
#
traffic classifier customer_B_pc operator and
 if-match customer-vlan-id 15 to 25
#
traffic classifier customer_B_voice operator and
 if-match customer-vlan-id 26 to 35
#
traffic classifier customer_B_storage operator and
 if-match customer-vlan-id 36 to 40
#
traffic behavior customer_A_pc
 nest top-most vlan 1001
 remark dot1p 3
#
traffic behavior customer_A_voice
```

```
 nest top-most vlan 1002
 remark dot1p 5
#
traffic behavior customer_A_video
 nest top-most vlan 1003
 remark dot1p 7
#
traffic behavior customer_B_pc
 nest top-most vlan 2001
 remark dot1p 3
#
traffic behavior customer_B_voice
 nest top-most vlan 2002
 remark dot1p 5
#
traffic behavior customer_B_storage
 nest top-most vlan 2003
 remark dot1p 7
#
qos policy customer_A
 classifier customer_A_pc behavior customer_A_pc
 classifier customer_A_voice behavior customer_A_voice
 classifier customer_A_video behavior customer_A_video
#
qos policy customer_B
 classifier customer_B_pc behavior customer_B_pc
 classifier customer_B_voice behavior customer_B_voice
 classifier customer_B_storage behavior customer_B_storage
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2001 to 2003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_B inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 1001 to 1003 untagged
 qinq enable
 qos trust dot1p
 qos apply policy customer_A inbound
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001 to 1003 2001 to 2003
#
```

Example: Configuring one-to-one VLAN mapping

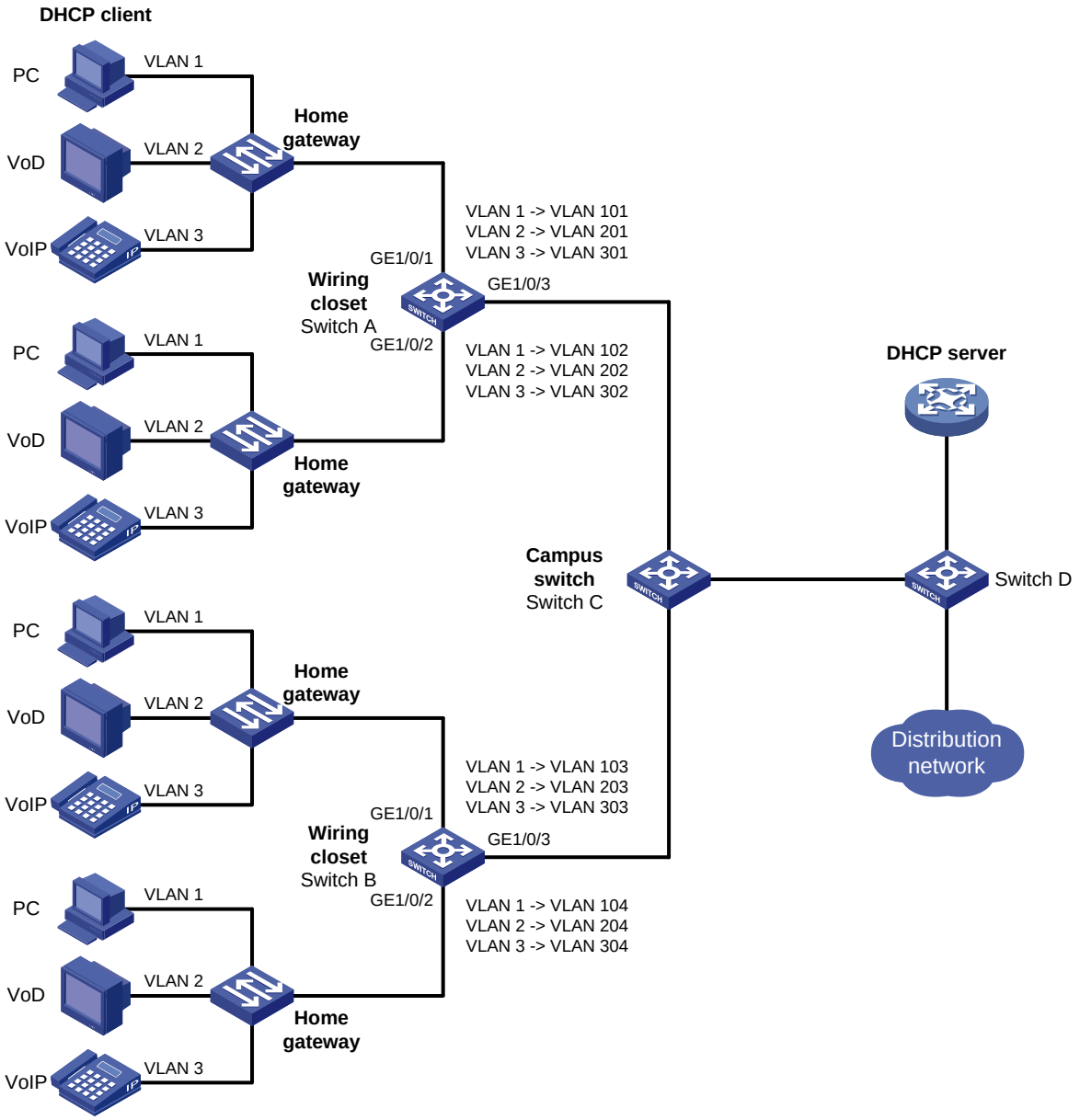
Network configuration

As shown in Figure 6:

- Each household subscribes to PC, VoD, and VoIP services, and obtains the IP address through DHCP.
- On the home gateways, PC, VoD, and VoIP service traffic is assigned to VLANs 1, 2, and 3, respectively.

To isolate traffic of the same service type from different households, configure one-to-one VLAN mapping on the wiring-closet switches. This feature assigns one VLAN to each type of traffic from each household.

Figure 6 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

Hardware	Software version
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx, Release 65xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx, Release 65xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx

Hardware	Software version
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Switch A

Create the original VLANs 2 and 3. (VLAN 1 is the system default VLAN and already exists.)

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
```

Create the translated VLANs 101 through 102, 201 through 202, and 301 through 302.

```
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

Configure the customer-side port GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to the original VLANs and translated VLANs.

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 1 2 3 101 201 301
```

Configure one-to-one VLAN mapping on GigabitEthernet 1/0/1 to map VLANs 1, 2, and 3 to VLANs 101, 201, and 301, respectively.

```
[SwitchA-GigabitEthernet1/0/1] vlan mapping 1 translated-vlan 101
[SwitchA-GigabitEthernet1/0/1] vlan mapping 2 translated-vlan 201
[SwitchA-GigabitEthernet1/0/1] vlan mapping 3 translated-vlan 301
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure the customer-side port GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to the original VLANs and translated VLANs.

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 1 2 3 102 202 302
```

Configure one-to-one VLAN mapping on GigabitEthernet 1/0/2 to map VLANs 1, 2, and 3 to VLANs 102, 202, and 302, respectively.

```
[SwitchA-GigabitEthernet1/0/2] vlan mapping 1 translated-vlan 102
[SwitchA-GigabitEthernet1/0/2] vlan mapping 2 translated-vlan 202
[SwitchA-GigabitEthernet1/0/2] vlan mapping 3 translated-vlan 302
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure the network-side port GigabitEthernet 1/0/3 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
```

Remove GigabitEthernet 1/0/3 from VLAN 1 and assign GigabitEthernet 1/0/3 to the translated VLANs.

```
[SwitchA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 101 201 301 102 202 302
[SwitchA-GigabitEthernet1/0/3] quit
```

Configuring Switch B

Configure Switch B in the same way Switch A is configured. (Details not shown.)

Verifying the configuration

Verify VLAN mapping information on the wiring-closet switches, for example, Switch A.

```
[SwitchA] display vlan mapping
Interface gigabitethernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           101                      N/A
  2             N/A           201                      N/A
  3             N/A           301                      N/A
Interface gigabitethernet1/0/2:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  1             N/A           102                      N/A
  2             N/A           202                      N/A
  3             N/A           302                      N/A
```

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2 to 3
#
vlan 101 to 102
#
vlan 201 to 202
#
vlan 301 to 302
#
interface gigabitethernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 3 101 201 301
 vlan mapping 1 translated-vlan 101
 vlan mapping 2 translated-vlan 201
 vlan mapping 3 translated-vlan 301
#
interface gigabitethernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 3 102 202 302
 vlan mapping 1 translated-vlan 102
 vlan mapping 2 translated-vlan 202
 vlan mapping 3 translated-vlan 302
#
interface gigabitethernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 101 to 102 201 to 202 301 to 302
#
```

- Switch B:

```
#
vlan 1
#
vlan 2 to 3
#
vlan 103 to 104
#
vlan 203 to 204
#
vlan 303 to 304
#
interface gigabitethernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 3 103 203 303
 vlan mapping 1 translated-vlan 103
```

```
 vlan mapping 2 translated-vlan 203
 vlan mapping 3 translated-vlan 303
#
interface gigabitethernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 3 104 204 304
 vlan mapping 1 translated-vlan 104
 vlan mapping 2 translated-vlan 204
 vlan mapping 3 translated-vlan 304
#
interface gigabitethernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 103 to 104 203 to 204 303 to 304
#
```

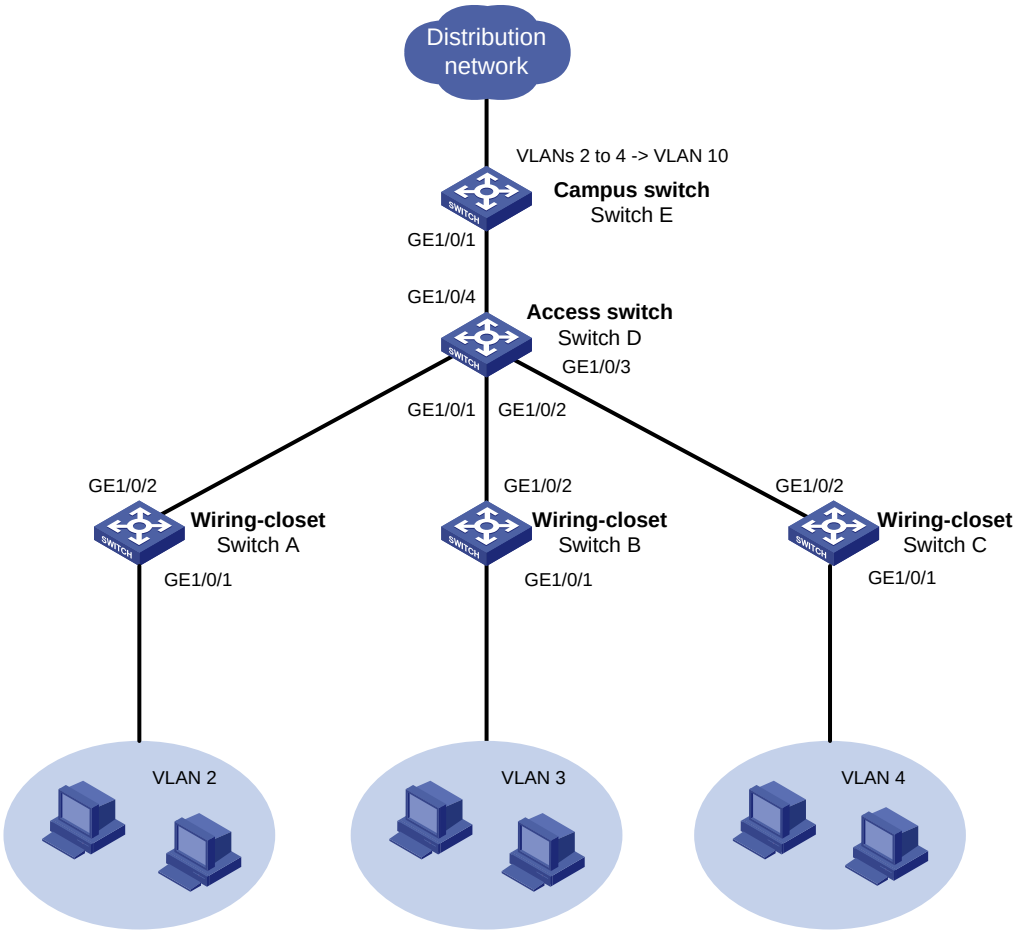
Example: Configuring many-to-one VLAN mapping

Network configuration

As shown in Figure 7:

- Create VLAN 2, VLAN 3, and VLAN 4 on the wiring-closet switches to isolate traffic of the same service type from different households.
- Configure many-to-one VLAN mappings on the campus switch. This feature assigns the same type of traffic from different households to one VLAN.

Figure 7 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-54C switch	
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series	Not supported
S5000E-X switch series	Not supported

Hardware	Software version
S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Switch A

Create VLAN 2 as an original VLAN.

```
<SwitchA> system-view
[SwitchA] vlan 2
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to VLAN 2.

```
[SwitchA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchA-if-range] port access vlan 2
```

Configuring Switch B and Switch C

Configure Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

Configuring Switch D

Create VLANs 2, 3, and 4 as original VLANs.

```
[SwitchD] vlan 2 to 4
```

Assign GigabitEthernet 1/0/1 to VLAN 2, GigabitEthernet 1/0/2 to VLAN 3, and GigabitEthernet 1/0/3 to VLAN 4.

```
[SwitchD] interface ten-gigabitethernet 1/0/1
```

```
[SwitchD-GigabitEthernet1/0/1] port access vlan 2
[SwitchD-GigabitEthernet1/0/1] quit
[SwitchD] interface ten-gigabitethernet 1/0/2
[SwitchD-GigabitEthernet1/0/2] port access vlan 3
[SwitchD-GigabitEthernet1/0/2] quit
[SwitchD] interface ten-gigabitethernet 1/0/3
[SwitchD-GigabitEthernet1/0/3] port access vlan 4
[SwitchD-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 as a trunk port and assign it to the original VLANs.

```
[SwitchD] interface ten-gigabitethernet 1/0/4
[SwitchD-GigabitEthernet1/0/4] port link-type trunk
[SwitchD-GigabitEthernet1/0/4] port trunk permit vlan 2 to 4
```

Configuring Switch E

Configure the customer-side port (GigabitEthernet 1/0/1) as a trunk port, and assign it to the original VLANs.

```
[SwitchE] interface gigabitethernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] port link-type trunk
[SwitchE-GigabitEthernet1/0/1] port trunk permit vlan 2 to 4
```

Configure many-to-one VLAN mapping on GigabitEthernet 1/0/1, which replaces VLAN tag 2 through VLAN tag 4 with VLAN tag 10.

```
[SwitchE-GigabitEthernet1/0/1] vlan mapping uni range 2 to 4 translated-vlan 10
```

Verifying the configuration

Verify VLAN mapping information on Switch E.

```
[SwitchE] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  2-4           N/A           10                       N/A
```

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- Switch B:

```
#
vlan 1
#
vlan 3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
```

- Switch C:

```
#
vlan 1
#
vlan 4
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4
#
```

- Switch D:

```
#
vlan 1
#
vlan 2 to 4
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/4
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 1 to 4
#
```

- Switch E:

```
#
vlan 1
#
vlan 2 to 4
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 4
 vlan mapping uni range 2 to 4 translated-vlan 10
#
```

Example: Configuring two-to-two VLAN mapping

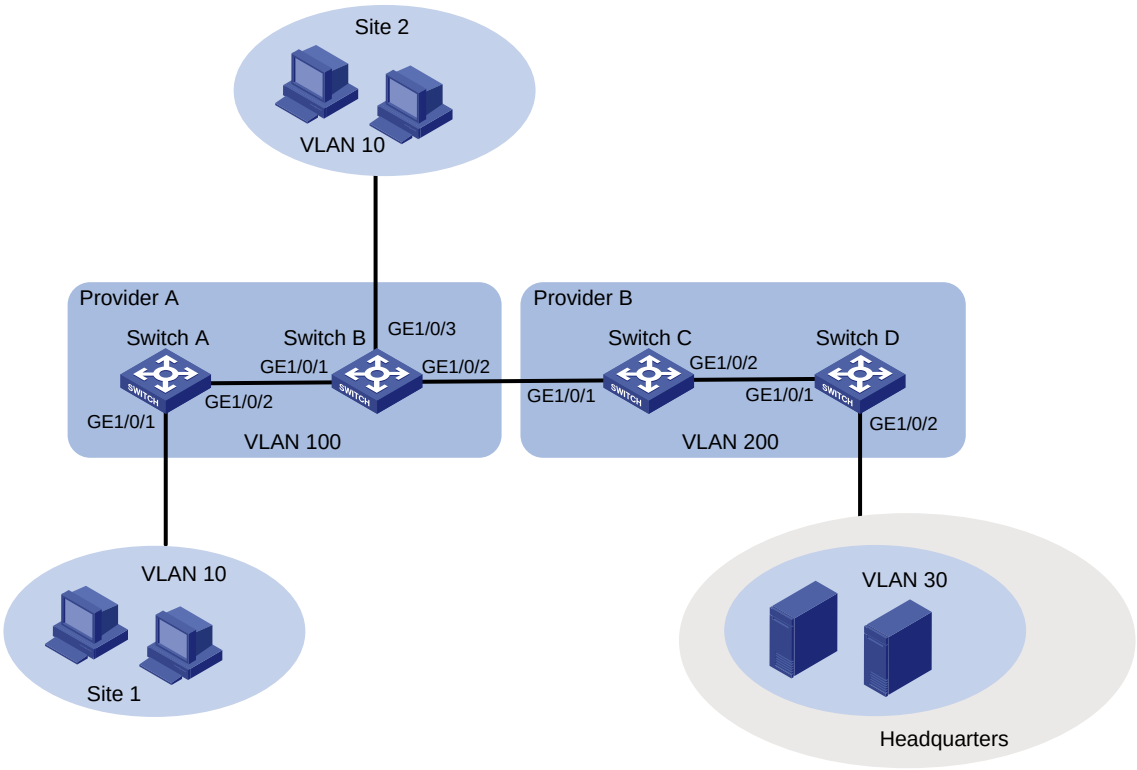
Network configuration

As shown in Figure 8:

- A company assigns its branch sites (Site 1 and Site 2) to VLAN 10, and the headquarters provides services in VLAN 30.
- Service provider A uses SVLAN 100 to transmit VLAN 10 traffic for the branch sites.
- Service provider B uses SVLAN 200 to transmit VLAN 30 traffic for the headquarters.

Configure two-to-two VLAN mapping to permit the two branch sites to access VLAN 30 of the headquarters without changing their VLAN assignment.

Figure 8 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6520X-EI switch series	
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch	Not supported

Hardware	Software version
E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

Configure two-to-two VLAN mapping on one of the edge devices between the two service provider networks. This example uses Switch C.

Procedures

Configuring Switch A

Create CVLAN 10 and SVLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] vlan 100
[SwitchA-vlan100] quit
```

Configure a one-to-two VLAN mapping on the customer-side port (GigabitEthernet 1/0/1) to add SVLAN tag 100 to packets from VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] vlan mapping nest single 10 nested-vlan 100
```

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
```

Assign GigabitEthernet 1/0/1 to VLAN 10 as a tagged member.

```
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
```

Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member.

```
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/1] undo port hybrid vlan 1
[SwitchA-GigabitEthernet1/0/1] quit
```

Configure the network-side port GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 100.

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring Switch B

Create CVLAN 10 and SVLAN 100.

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] vlan 100
[SwitchB-vlan100] quit
```

Configure a one-to-two VLAN mapping on the customer-side port (GigabitEthernet 1/0/3) to add SVLAN tag 100 to packets from VLAN 10.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] vlan mapping nest single 10 nested-vlan 100
```

Configure GigabitEthernet 1/0/3 as a hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
```

Assign GigabitEthernet 1/0/3 to VLAN 10 as a tagged member.

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 tagged
```

Assign GigabitEthernet 1/0/3 to VLAN 100 as an untagged member.

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 100 untagged
```

Remove GigabitEthernet 1/0/3 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/3] undo port hybrid vlan 1
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLAN 100.

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 100.

```
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 100
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchB-GigabitEthernet1/0/2] quit
```

Configuring Switch C

Create SVLANs 100 and 200.

```
<SwitchC> system-view
[SwitchC] vlan 100
[SwitchC-vlan100] quit
[SwitchC] vlan 200
[SwitchC-vlan200] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLANs 100 to 200.

```
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure a two-to-two VLAN mapping on GigabitEthernet 1/0/1 to map SVLAN 100 and CVLAN 10 to SVLAN 200 and CVLAN 30.

```
[SwitchC-GigabitEthernet1/0/1] vlan mapping tunnel 100 10 translated-vlan 200 30
[SwitchC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
```

Assign GigabitEthernet 1/0/2 to VLAN 200.

```
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 200
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/2] quit
```

Configuring Switch D

Create CVLAN 30 and SVLAN 200.

```
<SwitchD> system-view
[SwitchD] vlan 30
[SwitchD-vlan30] quit
[SwitchD] vlan 200
[SwitchD-vlan200] quit
```

Configure the link type of GigabitEthernet 1/0/1 as trunk.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
```

Assign GigabitEthernet 1/0/1 to VLAN 200.

```
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 200
```

Remove GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a hybrid port.

```
[SwitchD] interface gigabitethernet 1/0/2
[SwitchD-GigabitEthernet1/0/2] port link-type hybrid
```

Assign GigabitEthernet 1/0/2 to VLAN 30 as a tagged member.

```
[SwitchD-GigabitEthernet1/0/2] port hybrid vlan 30 tagged
```

Assign GigabitEthernet 1/0/2 to VLAN 200 as an untagged member.

```
[SwitchD-GigabitEthernet1/0/2] port hybrid vlan 200 untagged
```

Remove GigabitEthernet 1/0/2 from VLAN 1.

```
[SwitchD-GigabitEthernet1/0/2] undo port hybrid vlan 1
[SwitchD-GigabitEthernet1/0/2] quit
```

Configure a one-to-two VLAN mapping on the customer-side port (GigabitEthernet 1/0/2) to add SVLAN tag 200 to packets from VLAN 30.

```
[SwitchD] interface gigabitethernet 1/0/2
[SwitchD-GigabitEthernet1/0/2] vlan mapping nest single 30 nested-vlan 200
[SwitchD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify VLAN mapping information on Switch C.

```
[SwitchC] display vlan mapping
Interface GigabitEthernet1/0/1:
  Outer VLAN    Inner VLAN    Translated Outer VLAN    Translated Inner VLAN
  100           10            200                      30
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
vlan 10
vlan 100
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 100 untagged
 vlan mapping nest single 10 nested-vlan 100
#
interface GigabitEthernet1/0/2
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```

- Switch B:

```
#
vlan 10
vlan 100
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
#
interface GigabitEthernet1/0/3
 port link-type hybrid
 port hybrid vlan 10 tagged
 port hybrid vlan 100 untagged
 vlan mapping nest single 10 nested-vlan 100
```

- Switch C:

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 vlan mapping tunnel 100 10 translated-vlan 200 30
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200
#
```

- Switch D:

```
#
vlan 30
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 200
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 port hybrid vlan 30 tagged
 port hybrid vlan 200 untagged
 vlan mapping nest single 30 nested-vlan 200
#
```

Example: Modifying the CVLAN ID through QoS marking

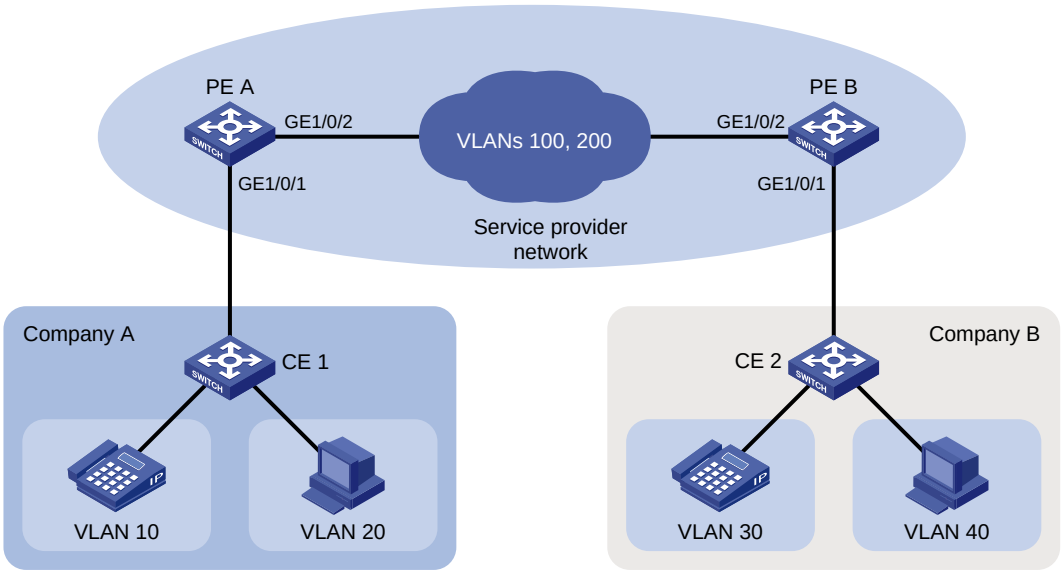
Network configuration

As shown in Figure 9:

- Company A uses CVLANs 10 and 20 to transmit voice traffic and data traffic, respectively.
- Company B uses CVLANs 30 and 40 to transmit voice traffic and data traffic, respectively.
- The service provider uses SVLANs 100 and 200 to transmit these two companies' voice and data traffic, respectively.

To provide Layer 2 connectivity for the voice and data traffic between the two companies, configure QoS CVLAN marking on PE A and PE B.

Figure 9 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To add different SVLAN tags to voice and data traffic, use the nest action for SVLAN tagging on the customer-side ports of PE A and PE B.

- To provide Layer 2 connectivity for the traffic from different CVLANs, configure QoS CVLAN marking on the service provider-side ports of PE A and PE B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported

Hardware	Software version
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4520V2 switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring PE A

1. Create the CVLANs and SVLANs.

```
<PE_A> system-view
[PE_A] vlan 10
[PE_A-vlan10] quit
[PE_A] vlan 20
[PE_A-vlan20] quit
[PE_A] vlan 100
[PE_A-vlan100] quit
[PE_A] vlan 200
[PE_A-vlan200] quit
[PE_A] vlan 30
[PE_A-vlan30] quit
[PE_A] vlan 40
[PE_A-vlan40] quit
```

2. Configure the customer-side port GigabitEthernet1/0/1:

Configure the port as a hybrid port.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] port link-type hybrid
```

Configure the port as an untagged VLAN member of VLANs 100 and 200.

```
[PE_A-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/1] undo port hybrid vlan 1
[PE_A-GigabitEthernet1/0/1] quit
```

Create the class **A10** to match frames with CVLAN 10.

```
[PE_A] traffic classifier A10
[PE_A-classifier-A10] if-match customer-vlan-id 10
[PE_A-classifier-A10] quit
```

Configure the traffic behavior **P100** to tag packets with SVLAN 100.

```
[PE_A] traffic behavior P100
[PE_A-behavior-P100] nest top-most vlan 100
[PE_A-behavior-P100] quit
```

Create the class **A20** to match frames with CVLAN 20.

```
[PE_A] traffic classifier A20
[PE_A-classifier-A20] if-match customer-vlan-id 20
[PE_A-classifier-A20] quit
```

Configure the traffic behavior **P200** to tag packets with SVLAN 200.

```
[PE_A] traffic behavior P200
[PE_A-behavior-P200] nest top-most vlan 200
[PE_A-behavior-P200] quit
```

Create the QoS policy **qinq** to associate the traffic classes **A10** and **A20** with the traffic behaviors **P100** and **P200**, respectively.

```
[PE_A] qos policy qinq
[PE_A-qospolicy-qinq] classifier A10 behavior P100
[PE_A-qospolicy-qinq] classifier A20 behavior P200
[PE_A-qospolicy-qinq] quit
```

Enable QinQ in the port.

```
[PE_A-GigabitEthernet1/0/1] qinq enable
```

Apply the QoS policy to the inbound direction of the port.

```
[PE_A-GigabitEthernet1/0/1] qos apply policy qinq inbound
[PE_A-GigabitEthernet1/0/1] quit
```

3. Configure the service network-side port GigabitEthernet1/0/2:

Configure the port as a trunk port.

```
[PE_A] interface gigabitethernet 1/0/2
[PE_A-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLANs 100 and 200.

```
[PE_A-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Remove the port from VLAN 1.

```
[PE_A-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE_A-GigabitEthernet1/0/2] quit
```

Create the class **A100** to match frames with CVLAN 10 and SVLAN 100.

```
[PE_A] traffic classifier A100
[PE_A-classifier-A100] if-match customer-vlan-id 10
[PE_A-classifier-A100] if-match service-vlan-id 100
[PE_A-classifier-A100] quit
```

Configure the traffic behavior **T100** to mark matching traffic with CVLAN 30.

```
[PE_A] traffic behavior T100
[PE_A-behavior-T100] remark customer-vlan-id 30
[PE_A-behavior-T100] quit
```

Create the class **A200** to match frames with CVLAN 20 and SVLAN 200.

```
[PE_A] traffic classifier A200
[PE_A-classifier-A200] if-match customer-vlan-id 20
[PE_A-classifier-A200] if-match service-vlan-id 200
[PE_A-classifier-A200] quit
```

Configure the traffic behavior **T200** to mark matching traffic with CVLAN 40.

```
[PE_A] traffic behavior T200
[PE_A-behavior-T200] remark customer-vlan-id 40
[PE_A-behavior-T200] quit
```

Create the QoS policy **vlanmapping** to associate the traffic classes **A100** and **A200** with the traffic behaviors **T100** and **T200**, respectively.

```
[PE_A] qos policy vlanmapping
[PE_A-qospolicy-vlanmapping] classifier A100 behavior T100
[PE_A-qospolicy-vlanmapping] classifier A200 behavior T200
[PE_A-qospolicy-vlanmapping] quit
```

Apply the QoS policy to the outbound direction of the port.

```
[PE_A-GigabitEthernet1/0/2] qos apply policy vlanmapping outbound
[PE_A-GigabitEthernet1/0/2] quit
```

Configuring PE B

1. Create the CVLANs and SVLANs.

```
<PE_B> system-view
[PE_B] vlan 30
[PE_B-vlan30] quit
[PE_B] vlan 40
[PE_B-vlan40] quit
[PE_B] vlan 100
```

```
[PE_B-vlan100] quit
[PE_B] vlan 200
[PE_B-vlan200] quit
[PE_B] vlan 10
[PE_B-vlan10] quit
[PE_B] vlan 20
[PE_B-vlan20] quit
```

2. Configure the customer-side port GigabitEthernet1/0/1:

Configure the port as a hybrid port.

```
[PE_B] interface gigabitethernet 1/0/1
[PE_B-GigabitEthernet1/0/1] port link-type hybrid
```

Assign the port to VLANs 100 and 200 as an untagged VLAN member.

```
[PE_B-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/1] undo port hybrid vlan 1
[PE_B-GigabitEthernet1/0/1] quit
```

Create the class **A30** to match frames with CVLAN 30.

```
[PE_B] traffic classifier A30
[PE_B-classifier-A30] if-match customer-vlan-id 30
[PE_B-classifier-A30] quit
```

Configure the traffic behavior **P100** to tag packets with SVLAN 100.

```
[PE_B] traffic behavior P100
[PE_B-behavior-P100] nest top-most vlan 100
[PE_B-behavior-P100] quit
```

Create the class **A40** to match frames with CVLAN 40.

```
[PE_B] traffic classifier A40
[PE_B-classifier-A40] if-match customer-vlan-id 40
[PE_B-classifier-A40] quit
```

Configure the traffic behavior **P200** to tag packets with SVLAN 200.

```
[PE_B] traffic behavior P200
[PE_B-behavior-P200] nest top-most vlan 200
[PE_B-behavior-P200] quit
```

Create the QoS policy **qinq** to associate the traffic classes **A30** and **A40** with the traffic behaviors **P100** and **P200**, respectively.

```
[PE_B] qos policy qinq
[PE_B-qospolicy-qinq] classifier A30 behavior P100
[PE_B-qospolicy-qinq] classifier A40 behavior P200
[PE_B-qospolicy-qinq] quit
```

Enable QinQ on the port.

```
[PE_B-GigabitEthernet1/0/1] qinq enable
```

Apply the QoS policy to the inbound direction of the port.

```
[PE_B-GigabitEthernet1/0/1] qos apply policy qinq inbound
[PE_B-GigabitEthernet1/0/1] quit
```

3. Configure the service provider-side port GigabitEthernet 1/0/2:

Configure the port as a trunk port.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLANs 100 and 200.

```
[PE_B-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Remove the port from VLAN 1.

```
[PE_B-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE_B-GigabitEthernet1/0/2] quit
```

Create the class **A100** to match frames with CVLAN 30 and SVLAN 100.

```
[PE_B] traffic classifier A100
[PE_B-classifier-A100] if-match customer-vlan-id 30
[PE_B-classifier-A100] if-match service-vlan-id 100
[PE_B-classifier-A100] quit
```

Configure the traffic behavior **T100** to mark matching traffic with CVLAN 10.

```
[PE_B] traffic behavior T100
[PE_B-behavior-T100] remark customer-vlan-id 10
[PE_B-behavior-T100] quit
```

Create the class **A200** to match frames with CVLAN 40 and SVLAN 200.

```
[PE_B] traffic classifier A200
[PE_B-classifier-A200] if-match customer-vlan-id 40
[PE_B-classifier-A200] if-match service-vlan-id 200
[PE_B-classifier-A200] quit
```

Configure the traffic behavior **T200** to mark matching traffic with CVLAN 20.

```
[PE_B] traffic behavior T200
[PE_B-behavior-T200] remark customer-vlan-id 20
[PE_B-behavior-T200] quit
```

Create the QoS policy **vlanmapping** to associate the traffic classes **A100** and **A200** with the traffic behaviors **T100** and **T200**, respectively.

```
[PE_B] qos policy vlanmapping
[PE_B-qospolicy-vlanmapping] classifier A100 behavior T100
[PE_B-qospolicy-vlanmapping] classifier A200 behavior T200
[PE_B-qospolicy-vlanmapping] quit
```

Apply the QoS policy to the outbound direction of the port.

```
[PE_B] interface gigabitethernet 1/0/2
[PE_B-GigabitEthernet1/0/2] qos apply policy vlanmapping outbound
[PE_B-GigabitEthernet1/0/2] quit
```

Configuring devices between PE A and PE B

Set the MTU to a minimum of 1504 bytes for each port on the path of double-tagged frames. (Details not shown.)

Configure the ports between PE A and PE B to allow frames from VLANs 100 and 200 to pass through tagged. (Details not shown.)

Verifying the configuration

Verify configuration on the customer-side ports on PE A and PE B. This example uses GigabitEthernet 1/0/1 of PE A.

```
[PE_A] interface gigabitethernet 1/0/1
[PE_A-GigabitEthernet1/0/1] display this
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 200 untagged
 qinq enable
 qos apply policy qinq inbound
#
return
```

Verify the QoS nesting configuration on the customer-side ports on PE A and PE B. This example uses GigabitEthernet 1/0/1 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/1

Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: qinq
   Classifier: A10
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 10
     Behavior: P100
      Nesting:
        Nest top-most vlan-id 100
   Classifier: A20
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 20
     Behavior: P200
      Nesting:
        Nest top-most vlan-id 200
```

Verify the QoS marking configuration on the service provider-side ports on PE A and PE B. This example uses GigabitEthernet 1/0/2 of PE A.

```
[PE_A] display qos policy interface gigabitethernet 1/0/2

Interface: GigabitEthernet1/0/2

  Direction: Outbound

  Policy: vlanmapping
   Classifier: A100
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 10
      If-match service-vlan-id 100
     Behavior: T100
      Marking:
```

```
      Remark Customer VLAN ID 30
Classifier: A200
  Operator: AND
  Rule(s) :
   If-match customer-vlan-id 20
   If-match service-vlan-id 200
  Behavior: T200
   Marking:
     Remark Customer VLAN ID 40
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- PE A:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan 100
#
vlan 200
#
traffic classifier A10 operator and
 if-match customer-vlan-id 10
#
traffic classifier A20 operator and
 if-match customer-vlan-id 20
#
traffic classifier A100 operator and
 if-match customer-vlan-id 10
 if-match service-vlan-id 100
#
traffic classifier A200 operator and
 if-match customer-vlan-id 20
 if-match service-vlan-id 200
#
traffic behavior P100
 nest top-most vlan 100
#
traffic behavior P200
 nest top-most vlan 200
```

```
#
traffic behavior T100
 remark customer-vlan-id 30
#
traffic behavior T200
 remark customer-vlan-id 40
#
qos policy qinq
 classifier A10 behavior P100
 classifier A20 behavior P200
#
qos policy vlanmapping
 classifier A100 behavior T100
 classifier A200 behavior T200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 200 untagged
 qinq enable
 qos apply policy qinq inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 qos apply policy vlanmapping outbound
#
```

- PE B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan 100
#
vlan 200
#
traffic classifier A30 operator and
 if-match customer-vlan-id 30
#
traffic classifier A40 operator and
```

```
 if-match customer-vlan-id 40
#
traffic classifier A100 operator and
 if-match customer-vlan-id 30
 if-match service-vlan-id 100
#
traffic classifier A200 operator and
 if-match customer-vlan-id 40
 if-match service-vlan-id 200
#
traffic behavior P100
 nest top-most vlan 100
#
traffic behavior P200
 nest top-most vlan 200
#
traffic behavior T100
 remark customer-vlan-id 10
#
traffic behavior T200
 remark customer-vlan-id 20
#
qos policy qinq
 classifier A30 behavior P100
 classifier A40 behavior P200
#
qos policy vlanmapping
 classifier A100 behavior T100
 classifier A200 behavior T200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 100 200 untagged
 qinq enable
 qos apply policy qinq inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 qos apply policy vlanmapping outbound
#
```

Contents

Introduction

This document provides DHCP snooping configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of DHCP.

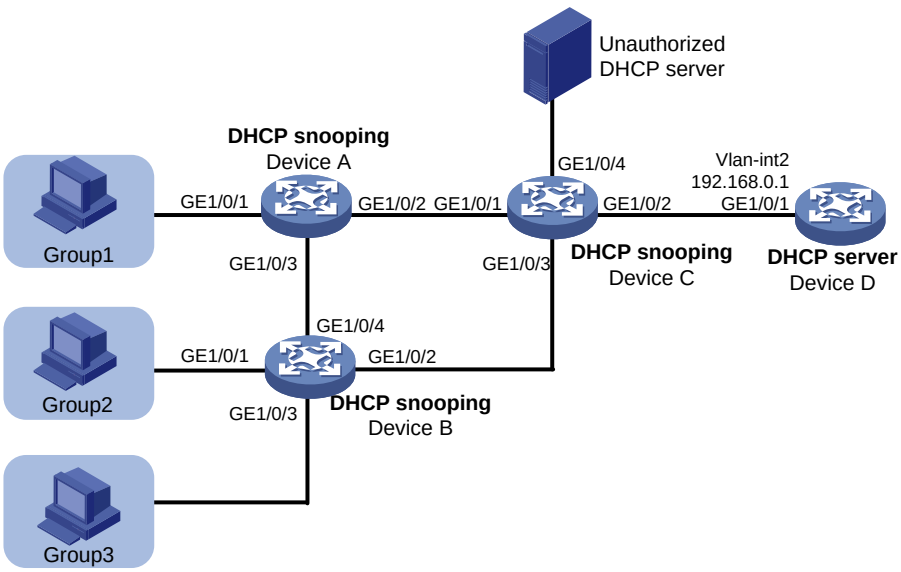
Example: Configuring DHCP snooping

Network configuration

As shown in Figure 1, three groups of hosts are connected to the DHCP server through the DHCP snooping devices. Configure DHCP snooping and DHCP server to meet the following requirements:

- Hosts in each group obtain IP addresses from the address range assigned to the group. Assign address ranges to the groups as follows:
  - Address range 192.168.0.2 to 192.168.0.39 for Group 1.
  - Address range 192.168.0.40 to 192.168.0.99 for Group 2.
  - Address range 192.168.0.100 to 192.168.0.200 for Group 3.
- The hosts can obtain IP addresses only from the authorized DHCP server.
- The hosts cannot access the network through IP addresses that are manually configured.

Figure 1 Network diagram

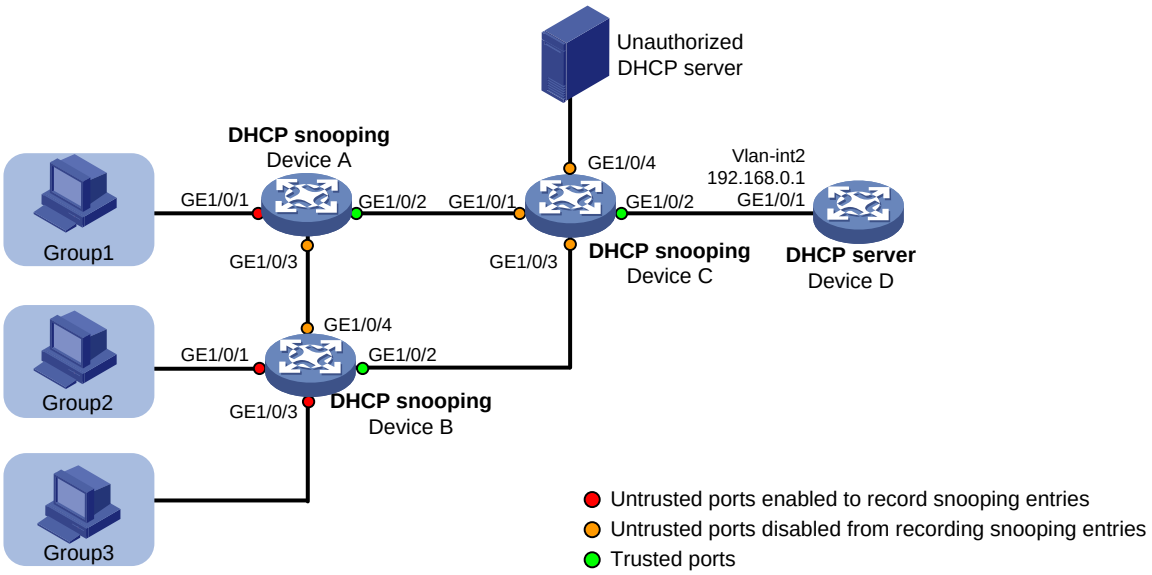


Analysis

To meet the network requirements, you must perform the following tasks:

- To make sure the hosts in each group obtain IP addresses from the address range assigned to the group, perform the following tasks:
  - Configure Option 82 on the DHCP snooping devices.
  - Create DHCP user classes for the groups and configure match rules based on Option 82 to match the groups on the DHCP server.
- To make sure the hosts obtain addresses only from the authorized DHCP server, configure ports facing the server as trusted and other ports as untrusted, as shown in Figure 2.
- To prevent illegal users from using manually configured IP addresses to access the network, perform the following tasks:
  - Enable ARP detection in the VLANs where the groups reside to check user validity based on DHCP snooping entries.
  - Enable recording of client information in DHCP snooping entries. To save system resources, you can enable only untrusted ports directly connected to hosts to record DHCP snooping entries, as shown in Figure 2.

Figure 2 Trusted and untrusted ports



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

The S5110V2-SI, S5000V3-EI, S5000V5-EI, S5000E-X, and WAS6000 switch series do not support the DHCP server.

Restrictions and guidelines

To ensure correct DHCP address allocation by using Option 82, you must perform Option 82 configuration on the DHCP server and the DHCP snooping devices.

Procedures

Configuring Device A

Enable DHCP snooping.

```
<DeviceA> system-view
[DeviceA] dhcp snooping enable
```

Enable recording of client information in DHCP snooping entries on interface GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on GigabitEthernet 1/0/1. Configure the padding content for the Circuit ID sub-option as **group1**.

```
[DeviceA-GigabitEthernet1/0/1] dhcp snooping information enable
[DeviceA-GigabitEthernet1/0/1] dhcp snooping information circuit-id string group1
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trusted port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable ARP attack detection for user validity check.

```
[DeviceA] vlan 1
[DeviceA-vlan1] arp detection enable
[DeviceA-vlan1] quit
```

Configure GigabitEthernet 1/0/2 as an ARP trusted port. By default, an interface is an ARP untrusted port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] arp detection trust
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B

Enable DHCP snooping.

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
```

Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on interface GigabitEthernet 1/0/1. Configure the padding content for the Circuit ID sub-option as **group2**.

```
[DeviceB-GigabitEthernet1/0/1] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/1] dhcp snooping information circuit-id string group2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure gigabitethernet 1/0/2 as a trusted port.

```
[DeviceB] interface GigabitEthernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/2] quit
```

Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping binding record
```

Enable DHCP snooping to support Option 82 on GigabitEthernet 1/0/3. Configure the padding content for the Circuit ID sub-option as **group3**.

```
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information enable
[DeviceB-GigabitEthernet1/0/3] dhcp snooping information circuit-id string group3
[DeviceB-GigabitEthernet1/0/3] quit
```

Enable ARP attack detection for user validity check.

```
[DeviceB] vlan 1
[DeviceB-vlan1] arp detection enable
[DeviceB-vlan1] quit
```

Configure GigabitEthernet 1/0/2 as an ARP trusted port. By default, an interface is an ARP untrusted port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp detection trust
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Enable DHCP snooping.

```
<DeviceC> system-view
[DeviceC] dhcp snooping enable
```

Configure GigabitEthernet 1/0/2 as a trusted port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] dhcp snooping trust
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

Assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceD> system-view
[DeviceD] vlan 2
[DeviceD-vlan2] port gigabitethernet 1/0/1
[DeviceD-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] ip address 192.168.0.1 24
[DeviceD-Vlan-interface2] quit
```

Enable DHCP.

```
[DeviceD] dhcp enable
```

Enable DHCP server on VLAN-interface 2.

```
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] dhcp select server
[DeviceD-Vlan-interface2] quit
```

Create DHCP user class **group1** for hosts in Group 1. Configure a match rule to match DHCP requests in which the third to eighth bytes of Option 82 is 0x67726F757031. The string 0x67726F757031 indicates that the content of the Circuit ID sub-option is **group1**.

```
[DeviceD] dhcp class group1
[DeviceD-dhcp-class-group1] if-match option 82 hex 67726F757031 offset 2 length 6
[DeviceD-dhcp-class-group1] quit
```

Create DHCP user class **group2** for hosts in Group 2. Configure a match rule to match DHCP requests in which the third to eighth bytes of Option 82 is 0x67726F757032. The string 0x67726F757032 indicates that the content of the Circuit ID sub-option is **group2**.

```
[DeviceD] dhcp class group2
[DeviceD-dhcp-class-group2] if-match option 82 hex 67726F757032 offset 2 length 6
[DeviceD-dhcp-class-group2] quit
```

Create DHCP user class **group3** for hosts in Group 3. Configure a match rule to match DHCP requests in which the third to eighth bytes of Option 82 is 0x67726F757033. The string 0x67726F757033 indicates that the content of the Circuit ID sub-option is **group3**.

```
[DeviceD] dhcp class group3
[DeviceD-dhcp-class-group3] if-match option 82 hex 67726F757033 offset 2 length 6
[DeviceD-dhcp-class-group3] quit
```

Create a DHCP address pool.

```
[DeviceD] dhcp server ip-pool 1
```

Specify the subnet for dynamic address allocation.

```
[DeviceD-dhcp-pool-1] network 192.168.0.0 mask 255.255.255.0
```

Specify address range 192.168.0.2 to 192.168.0.39 for DHCP user class **group1**.

```
[DeviceD-dhcp-pool-1] class group1 range 192.168.0.2 192.168.0.39
```

Specify address range 192.168.0.40 to 192.168.0.99 for DHCP user class **group2**.

```
[DeviceD-dhcp-pool-1] class group2 range 192.168.0.40 192.168.0.99
```

Specify address range 192.168.0.100 to 192.168.0.200 for DHCP user class **group3**.

```
[DeviceD-dhcp-pool-1] class group3 range 192.168.0.100 192.168.0.200
```

Apply the DHCP address pool to VLAN-interface 2.

```
[DeviceD] interface vlan-interface 2
[DeviceD-Vlan-interface2] dhcp server apply ip-pool 1
[DeviceD-Vlan-interface2] quit
```

Verifying the configuration

Verify that the hosts in each group can obtain IP addresses from the address range assigned to the group. This example uses a host in Group 2 to verify the configuration.

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter bb:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.0.44
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Manually assign IP address 192.168.0.66 to a host in Group 2, and verify that it cannot access the external network. (Details not shown.)

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 dhcp snooping enable
#
vlan 1
 arp detection enable
#
interface GigabitEthernet1/0/1
 dhcp snooping binding record
 dhcp snooping information enable
 dhcp snooping information circuit-id string group1
#
interface GigabitEthernet1/0/2
 arp detection trust
 dhcp snooping trust
#
```

- Device B:

```
#
 dhcp snooping enable
#
vlan 1
 arp detection enable
#
interface GigabitEthernet1/0/1
 dhcp snooping binding record
 dhcp snooping information enable
 dhcp snooping information circuit-id string group2
#
interface GigabitEthernet1/0/2
 arp detection trust
 dhcp snooping trust
#
interface GigabitEthernet1/0/3
 dhcp snooping binding record
 dhcp snooping information enable
 dhcp snooping information circuit-id string group3
#
```

- Device C:

```
#
 dhcp snooping enable
#
interface GigabitEthernet1/0/2
```

```
 dhcp snooping trust
#
```

- Device D:

```
#
 dhcp enable
#
vlan 2
#
dhcp class group1
 if-match option 82 hex 67726f757031 offset 2 length 6
#
dhcp class group2
 if-match option 82 hex 67726f757032 offset 2 length 6
#
dhcp class group3
 if-match option 82 hex 67726f757033 offset 2 length 6
#
dhcp server ip-pool 1
 network 192.168.0.0 mask 255.255.255.0
 class group1 range 192.168.0.2 192.168.0.39
 class group2 range 192.168.0.40 192.168.0.99
 class group3 range 192.168.0.100 192.168.0.200
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
 dhcp server apply ip-pool 1
#
```

Contents

Introduction

This document provides examples for configuring cross-subnet dynamic IP address allocation.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of DHCP.

Example: Configuring cross-subnet dynamic IP address allocation

Network configuration

As shown in Figure 1, a company's branches are on a different subnet from the headquarters. Device A acts as the gateway of the headquarters and Device B acts as the gateway for the branches.

Configure DHCP server on Device A to meet the following requirements:

- The hosts at the headquarters obtain IP addresses in the range of 10.1.1.2 to 10.1.1.100.
- The hosts at branch 1 obtain IP addresses in the range of 10.1.3.2 to 10.1.3.48. The hosts at branch 2 obtain IP addresses in the range of 10.1.3.49 to 10.1.3.100.
- The hosts at the headquarters and branches obtain the DNS server address, the TFTP server address, the domain name suffix, and the gateway address through DHCP.

Configure DHCP relay agent on Device B to meet the following requirements:

- The hosts at the branches obtain IP addresses and other configuration parameters from the DHCP server.
- The hosts at the branches cannot access the network by using manually configured IP addresses.
- The hosts at each branch obtain IP addresses from the address range assigned to the branch.

Figure 1 Network diagram

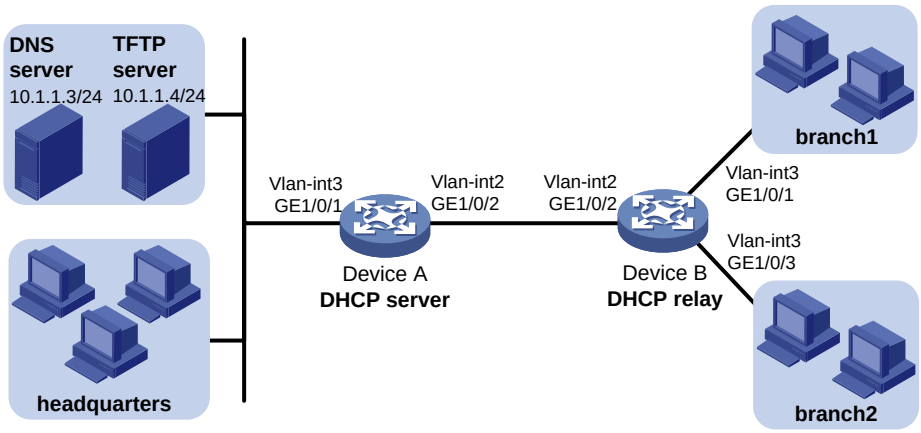


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int3	10.1.1.1/24	Device B	Vlan-int3	10.1.3.1/24
	Vlan-int2	10.1.2.1/24		Vlan-int2	10.1.2.2/24

Analysis

To meet the network requirements, you must perform the following tasks:

- Exclude the IP addresses of the DNS server and TFTP server from dynamic address allocation to prevent them from being assigned to hosts.
- To prevent the hosts at the branches from using manually configured IP addresses to access the network, perform the following tasks:
  - Enable the DHCP relay agent to record client information in DHCP relay entries.
  - Enable IP source guard to filter incoming packets based on the DHCP relay entries.
- To make sure the hosts in each branch obtain IP addresses from the address range assigned to the branch, perform the following tasks:
  - Configure Option 82 on the DHCP relay agent.
  - Create DHCP user classes for the branches and configure match rules based on Option 82 to match the branches on the DHCP server.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx

S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

To ensure correct DHCP address allocation by using Option 82, you must perform Option 82 configuration on both the DHCP server and the DHCP relay agent.

Procedures

Configuring Device A

Assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.2.1 24
[DeviceA-Vlan-interface2] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/1
[DeviceA-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 10.1.1.1 24
[DeviceA-Vlan-interface3] quit
```

Enable DHCP.

```
[DeviceA] dhcp enable
```

Enable DHCP server on VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] dhcp select server
[DeviceA-Vlan-interface2] quit
```

Enable DHCP server on VLAN-interface 3.

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] dhcp select server
[DeviceA-Vlan-interface3] quit
```

Create DHCP address pool 1.

```
[DeviceA] dhcp server ip-pool 1
```

Specify the subnet and address range for dynamic address allocation.

```
[DeviceA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] address range 10.1.1.2 10.1.1.100
```

Specify the DNS server address, TFTP server address, domain name suffix, and gateway address to be assigned to clients.

```
[DeviceA-dhcp-pool-1] dns-list 10.1.1.3
[DeviceA-dhcp-pool-1] tftp-server ip-address 10.1.1.4
[DeviceA-dhcp-pool-1] domain-name com
[DeviceA-dhcp-pool-1] gateway-list 10.1.1.1
```

Exclude the IP addresses of the DNS server and TFTP server from dynamic address allocation.

```
[DeviceA-dhcp-pool-1] forbidden-ip 10.1.1.3 10.1.1.4
[DeviceA-dhcp-pool-1] quit
```

Apply the DHCP address pool to VLAN-interface 3.

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] dhcp server apply ip-pool 1
[DeviceA-Vlan-interface3] quit
```

Create DHCP user class **aa** for the hosts at branch 1. Configure a match rule to match DHCP requests in which the fifth and sixth bytes of Option 82 are 0x0001. The string 0x0001 indicates that the clients are connected to interface GigabitEthernet 1/0/1.

```
[DeviceA] dhcp class aa
[DeviceA-dhcp-class-aa] if-match option 82 hex 0001 offset 4 length 2
[DeviceA-dhcp-class-aa] quit
```

Create DHCP user class **bb** for the hosts at branch 2. Configure a match rule to match DHCP requests in which the fifth and sixth bytes of Option 82 are 0x0003. The string 0x0003 indicates that the clients are connected to interface GigabitEthernet 1/0/3.

```
[DeviceA] dhcp class bb
[DeviceA-dhcp-class-bb] if-match option 82 hex 0003 offset 4 length 2
[DeviceA-dhcp-class-bb] quit
```

Create DHCP address pool 2.

```
[DeviceA] dhcp server ip-pool 2
```

Specify the subnet for dynamic address allocation.

```
[DeviceA-dhcp-pool-2] network 10.1.3.0 mask 255.255.255.0
```

Specify address range 10.1.3.2 to 10.1.3.48 for DHCP user class **aa**.

```
[DeviceA-dhcp-pool-2] class aa range 10.1.3.2 10.1.3.48
```

Specify address range 10.1.3.49 to 10.1.3.100 for DHCP user class **bb**.

```
[DeviceA-dhcp-pool-2] class bb range 10.1.3.49 10.1.3.100
```

Specify the DNS server address, TFTP server address, domain name suffix, and gateway address to be assigned to clients.

```
[DeviceA-dhcp-pool-2] tftp-server ip-address 10.1.1.4
[DeviceA-dhcp-pool-2] dns-list 10.1.1.3
[DeviceA-dhcp-pool-2] domain-name com
[DeviceA-dhcp-pool-2] gateway-list 10.1.3.1
[DeviceA-dhcp-pool-2] quit
```

Apply the DHCP address pool to VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] dhcp server apply ip-pool 2
[DeviceA-Vlan-interface2] quit
```

Configure a static route to subnet 10.1.3.0/24.

```
[DeviceA] ip route-static 10.1.3.0 24 10.1.2.2
```

Configuring Device B

Assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 10.1.2.2 24
[DeviceB-Vlan-interface2] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to VLAN 3.

```
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/1
[DeviceB-vlan3] port gigabitethernet 1/0/3
[DeviceB-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 10.1.3.1 24
```

```
[DeviceB-Vlan-interface3] quit
```

Enable DHCP.

```
[DeviceB] dhcp enable
```

Enable DHCP relay agent on VLAN-interface 3.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] dhcp select relay
```

Specify the IP address of the DHCP server.

```
[DeviceB-Vlan-interface3] dhcp relay server-address 10.1.2.1
```

Enable the DHCP relay agent to support Option 82.

```
[DeviceB-Vlan-interface3] dhcp relay information enable
[DeviceB-Vlan-interface3] quit
```

Enable recording of client information in DHCP relay entries.

```
[DeviceB] dhcp relay client-information record
```

Enable IPv4 source guard on VLAN-interface 3 to filter incoming packets by source IPv4 addresses and source MAC addresses.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip verify source ip-address mac-address
[DeviceB-Vlan-interface3] quit
```

Configure a static route to subnet 10.1.1.0/24.

```
[DeviceB] ip route-static 10.1.1.0 24 10.1.2.1
```

Verifying the configuration

Verify that the IP address 10.1.3.3 has been assigned to a client.

```
<DeviceA> display dhcp server ip-in-use ip 10.1.3.3
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.3.3         0033-6365-352e-6136-  Jan  2 00:34:02 2016  Auto(C)
                 6466-2e65-3133-392d-
                 5465-6e2d-4769-6761-
                 6269-7445-7468-6572-
                 6e65-7431-2f30-2f35-
                 31
```

Verify that the hosts at each branch can obtain IP addresses from the address range assigned to the branch. This example uses a host at branch 2.

```
C:\Documents and Settings\aa>ipconfig

Windows IP Configuration

Ethernet adapter aa:

        Connection-specific DNS Suffix  . : domain-name com
        IP Address. . . . . . . . . . . . : 10.1.3.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IPv6 Address. . . . . . . . . . . : fe80::20f:3dff:fe80:2b38%4
        Default Gateway . . . . . . . . . : 10.1.3.1
```

Manually assign IP address 10.1.3.87 to a host at branch 2, and verify that the host cannot access the TFTP server. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 dhcp enable
#
vlan 2 to 3
#
dhcp class aa
 if-match option 82 hex 0001 offset 4 length 2
#
dhcp class bb
 if-match option 82 hex 0003 offset 4 length 2
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.0
 address range 10.1.1.2 10.1.1.100
 dns-list 10.1.1.3
 domain-name com
 forbidden-ip 10.1.1.3
 forbidden-ip 10.1.1.4
 gateway-list 10.1.1.1
 tftp-server ip-address 10.1.1.4
#
dhcp server ip-pool 2
 network 10.1.3.0 mask 255.255.255.0
 class aa range 10.1.3.2 10.1.3.48
 class bb range 10.1.3.49 10.1.3.100
 dns-list 10.1.1.3
 domain-name com
 gateway-list 10.1.3.1
 tftp-server ip-address 10.1.1.4
#
interface Vlan-interface2
 ip address 10.1.2.1 255.255.255.0
 dhcp server apply ip-pool 2
#
interface Vlan-interface3
 ip address 10.1.1.1 255.255.255.0
 dhcp server apply ip-pool 1
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
ip route-static 10.1.3.0 24 10.1.2.2
#
```

- Device B:

```
#
 dhcp enable
 dhcp relay client-information record
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.2.2 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.3.1 255.255.255.0
 dhcp select relay
 dhcp relay information enable
 dhcp relay server-address 10.1.2.1
 ip verify source ip-address mac-address
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
ip route-static 10.1.1.0 24 10.1.2.1
#
```

Contents

Introduction

This document provides IPv6 over IPv4 tunneling with OSPFv3 configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of HP IPv6 over IPv4 tunneling and OSPFv3.

Example: Configuring IPv6 over IPv4 tunneling with OSPFv3

Network configuration

As shown in Figure 1, in IPv6 networks, Device A, Device B, and Device C act as the gateways of the headquarters, Branch 1, and Branch 2, respectively.

Configure IPv6 over IPv4 tunnels to ensure that the headquarters can communicate with the two branches over IPv4 networks.

Configure OSPFv3 on the gateways to ensure the following:

- The gateways have routes to destination IPv6 addresses through tunnel interfaces.
- Branch 1 and Branch 2 can communicate with each other through the headquarters.

Figure 1 Network diagram

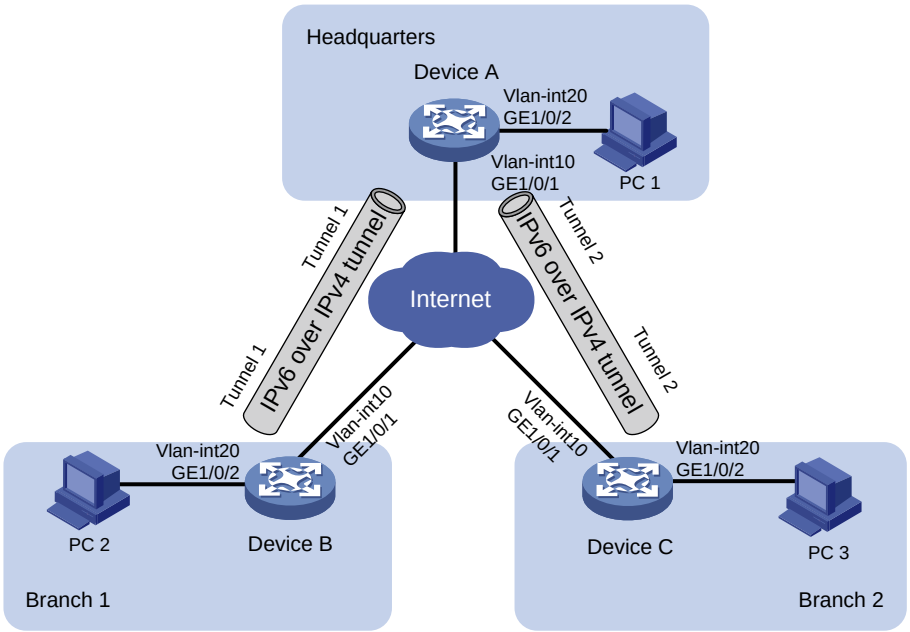


Table 1 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int10	20.1.1.1/24
	Vlan-int20	2001::1/64
	Tunnel1	3001::1/64
	Tunnel2	4001::1/64
Device B	Vlan-int10	30.1.1.1/24
	Vlan-int20	5001::1/64
	Tunnel1	3001::2/64
Device C	Vlan-int10	40.1.1.1/24
	Vlan-int20	6001::1/64
	Tunnel2	4001::2/64

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI, and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series	Not supported

Hardware	Software version
MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Make sure the gateways can reach each other at IPv4.

Configuring IPv6 over IPv4 tunnels

- Configure Device A:

  # Configure an IP address for VLAN-interface 10.

  ```
  <DeviceA> system-view
  [DeviceA] vlan 10
  [DeviceA-vlan10] port GigabitEthernet 1/0/1
  [DeviceA-vlan10] quit
  [DeviceA] interface vlan-interface 10
  [DeviceA-Vlan-interface10] ip address 20.1.1.1 24
  [DeviceA-Vlan-interface10] quit
  ```

  # Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

  # Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

  ```
  [DeviceA] service-loopback group 1 type tunnel
  [DeviceA] interface gigabitethernet 1/0/3
  [DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
  [DeviceA-GigabitEthernet1/0/3] quit
  ```

  # Configure an IPv6 over IPv4 tunnel interface Tunnel 1.

  ```
  [DeviceA] interface tunnel 1 mode ipv6-ipv4
  ```

  # Configure an IPv6 address for Tunnel 1.

  ```
  [DeviceA-Tunnel1] ipv6 address 3001::1/64
  ```

  # Specify VLAN-interface 10 as the source interface of Tunnel 1.

  ```
  [DeviceA-Tunnel1] source vlan-interface 10
  ```

  # Specify the destination address for Tunnel 1.

```
[DeviceA-Tunnel1] destination 30.1.1.1
[DeviceA-Tunnel1] quit
```

Configure an IPv6 over IPv4 tunnel interface Tunnel 2.

```
[DeviceA] interface tunnel 2 mode ipv6-ipv4
```

Configure an IPv6 address for Tunnel 2.

```
[DeviceA-Tunnel2] ipv6 address 4001::1/64
```

Specify VLAN-interface 10 as the source interface of Tunnel 2.

```
[DeviceA-Tunnel2] source Vlan-interface 10
```

Specify the destination address for Tunnel 2.

```
[DeviceA-Tunnel2] destination 40.1.1.1
[DeviceA-Tunnel2] quit
```

- Configure Device B:

  # Configure an IP address for VLAN-interface 10.

  ```
  <DeviceB> system-view
  [DeviceB] vlan 10
  [DeviceB-vlan10] port GigabitEthernet 1/0/1
  [DeviceB-vlan10] quit
  [DeviceB] interface vlan-interface 10
  [DeviceB-Vlan-interface10] ip address 30.1.1.1 24
  [DeviceB-Vlan-interface10] quit
  ```

  # Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

  # Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

  ```
  [DeviceB] service-loopback group 1 type tunnel
  [DeviceB] interface gigabitethernet 1/0/3
  [DeviceB-GigabitEthernet1/0/3] port service-loopback group 1
  [DeviceB-GigabitEthernet1/0/3] quit
  ```

  # Configure an IPv6 over IPv4 tunnel interface Tunnel 1.

  ```
  [DeviceB] interface tunnel 1 mode ipv6-ipv4
  ```

  # Configure an IPv6 address for Tunnel 1.

  ```
  [DeviceB-Tunnel1] ipv6 address 3001::2/64
  ```

  # Specify VLAN-interface 10 as the source interface of Tunnel 1.

  ```
  [DeviceB-Tunnel1] source vlan-interface 10
  ```

  # Specify the destination address for Tunnel 1.

  ```
  [DeviceB-Tunnel1] destination 20.1.1.1
  [DeviceB-Tunnel1] quit
  ```

- Configure Device C:

  # Configure an IP address for VLAN-interface 10.

  ```
  <DeviceC> system-view
  [DeviceC] vlan 10
  [DeviceC-vlan10] port GigabitEthernet 1/0/1
  [DeviceC-vlan10] quit
  [DeviceC] interface vlan-interface 10
  [DeviceC-Vlan-interface10] ip address 40.1.1.1 24
  [DeviceC-Vlan-interface10] quit
  ```

  # Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, and S5850 switch series to receive and send tunnel packets.)

```
[DeviceC] service-loopback group 1 type tunnel
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceC-GigabitEthernet1/0/3] quit
```

Configure an IPv6 over IPv4 tunnel interface Tunnel 2.

```
[DeviceC] interface tunnel 2 mode ipv6-ipv4
```

Configure an IPv6 address for Tunnel 2.

```
[DeviceC-Tunnel2] ipv6 address 4001::2/64
```

Specify VLAN-interface 10 as the source interface of Tunnel 2.

```
[DeviceC-Tunnel2] source vlan-interface 10
```

Specify the destination address for Tunnel 2.

```
[DeviceC-Tunnel2] destination 20.1.1.1
[DeviceC-Tunnel2] quit
```

Configuring OSPFv3

- Configure Device A:

  # Specify the router ID as 1.1.1.1.

  ```
  [DeviceA] ospfv3
  [DeviceA-ospfv3-1] router-id 1.1.1.1
  [DeviceA-ospfv3-1] quit
  ```

  # Enable OSPFv3 on Tunnel 1.

  ```
  [DeviceA] interface Tunnel 1
  [DeviceA-Tunnel1] ospfv3 1 area 0
  [DeviceA-Tunnel1] quit
  ```

  # Enable OSPFv3 on Tunnel 2.

  ```
  [DeviceA] interface Tunnel 2
  [DeviceA-Tunnel2] ospfv3 1 area 0
  [DeviceA-Tunnel2] quit
  ```

  # Enable OSPFv3 on VLAN-interface 20.

  ```
  [DeviceA] interface vlan-interface 20
  [DeviceA-Vlan-interface20] ospfv3 1 area 0
  [DeviceA-Vlan-interface20] quit
  ```

- Configure Device B:

  # Specify the router ID as 2.2.2.2.

  ```
  [DeviceB] ospfv3
  [DeviceB-ospfv3-1] router-id 2.2.2.2
  [DeviceB-ospfv3-1] quit
  ```

  # Enable OSPFv3 on Tunnel 1.

  ```
  [DeviceB] interface Tunnel 1
  [DeviceB-Tunnel1] ospfv3 1 area 0
  [DeviceB-Tunnel1] quit
  ```

  # Enable OSPFv3 on VLAN-interface 20.

  ```
  [DeviceB] interface vlan-interface 20
  ```

```
[DeviceB-Vlan-interface20] ospfv3 1 area 0
[DeviceB-Vlan-interface20] quit
```

- Configure Device C:

  # Specify the router ID as 3.3.3.3.

```
[DeviceC] ospfv3
[DeviceC-ospfv3-1] router-id 3.3.3.3
[DeviceC-ospfv3-1] quit
```

  # Enable OSPFv3 on Tunnel 2.

```
[DeviceC] interface Tunnel 2
[DeviceC-Tunnel2] ospfv3 1 area 0
[DeviceC-Tunnel2] quit
```

  # Enable OSPFv3 on VLAN-interface 20.

```
[DeviceC] interface vlan-interface 20
[DeviceC-Vlan-interface20] ospfv3 1 area 0
[DeviceC-Vlan-interface20] quit
```

Verifying the configuration

Ping PC 1 from PC 2.

```
D:\>ping6 -s 5001::3 2001::3

Pinging 2001::3
from 5001::3 with 32 bytes of data:

Reply from 2001::3: bytes=32 time=13ms
Reply from 2001::3: bytes=32 time=1ms
Reply from 2001::3: bytes=32 time=1ms
Reply from 2001::3: bytes=32 time<1ms

Ping statistics for 2001::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

The output shows that the ping operation succeeds.

Ping PC 3 from PC 2.

```
D:\>ping6 -s 5001::3 6001::3

Pinging 6001::3
from 6001::3 with 32 bytes of data:

Reply from 6001::3: bytes=32 time=13ms
Reply from 6001::3: bytes=32 time=1ms
Reply from 6001::3: bytes=32 time=1ms
Reply from 6001::3: bytes=32 time<1ms

Ping statistics for 6001::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

The output shows that the ping operation succeeds.

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 service-loopback group 1 type tunnel
#
ospfv3 1
 router-id 1.1.1.1
 area 0.0.0.0
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 20.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source Vlan-interface10
 destination 30.1.1.1
 ipv6 address 3001::1/64
#
interface Tunnel2 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
```

```
 source Vlan-interface10
 destination 40.1.1.1
 ipv6 address 4001::1/64
#
```

- Device B:

```
#
 service-loopback group 1 type tunnel
#
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 30.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 address 5001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source Vlan-interface10
 destination 20.1.1.1
 ipv6 address 3001::2/64
#
```

- Device C:

```
#
 service-loopback group 1 type tunnel
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
```

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 40.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 address 6001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel2 mode ipv6-ipv4
 ospfv3 1 area 0.0.0.0
 source Vlan-interface10
 destination 20.1.1.1
 ipv6 address 4001::2/64
#
```

Contents

Introduction

This document provides IPv6 over IPv4 GRE tunnel configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of GRE.

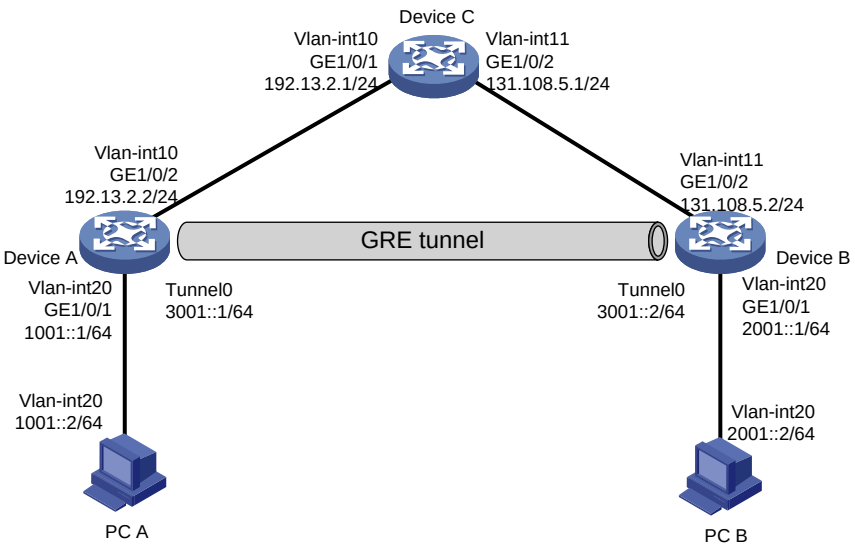
Example: Configuring an IPv6 over IPv4 GRE tunnel

Network configuration

As shown in Figure 1, Device A, Device B, and Device C are all on an IPv4 network. Dual stack devices Device A and Device B each connect to an IPv6 host.

Configure a GRE/IPv4 tunnel between Device A and Device B, so PC A and PC B can communicate with each other over the IPv4 network.

Figure 1 Network diagram



Analysis

To meet the network requirements, perform the following tasks:

- To enable the IPv6 hosts to communicate over the IPv4 network, specify the GRE tunnel mode as GRE/IPv4 and configure IPv6 addresses for the tunnel interfaces.

- To transmit packets between PC A and PC B through the GRE tunnel, configure a route reaching the destination network through the tunnel interface on Device A and Device B. You can configure the routes by using either of the following methods:
  - Configure static routes, using the peer tunnel interface as the next hop or using the local tunnel interface as the outgoing interface.
  - Enable a dynamic routing protocol on both the tunnel interfaces and the Layer 3 interfaces connected to PC A and PC B.
- For both ends of the GRE tunnel to reach each other, configure a static route reaching the remote end on Device A and Device B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx

Hardware	Software version
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch	Not supported

Hardware	Software version
IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

You must configure the tunnel source address and destination address at both ends of the tunnel. The tunnel source or destination address at one end must be the tunnel destination or source address at the other end.

Procedures

Configuring Device A

Configure VLAN-interface 20.

```
<DeviceA> system-view
[DeviceA] vlan 20
[DeviceA-vlan20] port GigabitEthernet 1/0/1
[DeviceA-vlan20] quit
[DeviceA] interface vlan-interface 20
[DeviceA-vlan-interface20] ipv6 address 1001::1 64
[DeviceA-vlan-interface20] quit
```

Configure other interfaces in the same way VLAN-interface 20 is configured. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceA] service-loopback group 1 type tunnel
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Create a tunnel interface named **Tunnel 0**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceA] interface tunnel 0 mode gre
```

Configure an IPv6 address for tunnel interface **Tunnel 0**.

```
[DeviceA-Tunnel0] ipv6 address 3001::1 64
```

Configure the source address of tunnel interface **Tunnel 0** as the IP address of VLAN-interface 10.

```
[DeviceA-Tunnel0] source 192.13.2.2
```

Configure the destination address of tunnel interface **Tunnel 0** as the IP address of VLAN-interface 11 on Device B.

```
[DeviceA-Tunnel0] destination 131.108.5.2
[DeviceA-Tunnel0] quit
```

Configure a static route reaching PC B through tunnel interface **Tunnel 0**.

```
[DeviceA] ipv6 route-static 2001:: 64 tunnel 0
```

Configure a static route reaching the remote end of the GRE tunnel.

```
[DeviceA] ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
```

Configuring Device B

Configure VLAN-interface 20.

```
<DeviceB> system-view
[DeviceB] vlan 20
[DeviceB-vlan20] port GigabitEthernet 1/0/1
[DeviceB] interface vlan-interface 20
[DeviceB-Vlan-interface20] ipv6 address 2001::1 64
[DeviceB-Vlan-interface20] quit
```

Configure other interfaces in the same way VLAN-interface 20 is configured. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceB] service-loopback group 1 type tunnel
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceB-GigabitEthernet1/0/3] quit
```

Create a tunnel interface named **Tunnel 0**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceB] interface tunnel 0 mode gre
```

Configure an IPv6 address for tunnel interface **Tunnel 0**.

```
[DeviceB-Tunnel0] ipv6 address 3001::2 64
```

Configure the source address of tunnel interface **Tunnel 0** as the IP address of VLAN-interface 11.

```
[DeviceB-Tunnel0] source 131.108.5.2
```

Configure the destination address of tunnel interface **Tunnel 0** as the IP address of VLAN-interface 10 on Device A.

```
[DeviceB-Tunnel0] destination 192.13.2.2
[DeviceB-Tunnel0] quit
```

Configure a static route reaching PC A through tunnel interface **Tunnel 0**.

```
[DeviceB] ipv6 route-static 1001:: 64 Tunnel 0
```

Configure a static route reaching the remote end of the GRE tunnel.

```
[DeviceB] ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
```

Configuring Device C

Configure VLAN-interface 10.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] port GigabitEthernet 1/0/1
[DeviceC-vlan10] quit
[DeviceC] interface Vlan-interface 10
[DeviceC-Vlan-interface10] ip address 192.13.2.1 24
[DeviceC-Vlan-interface10] quit
```

Configure VLAN-interface 11.

```
[DeviceC] vlan 11
```

```
[DeviceC-vlan11] port GigabitEthernet 1/0/2
[DeviceC-vlan11] quit
[DeviceC] interface vlan-interface 11
[DeviceC-Vlan-interface11] ip address 131.108.5.1 24
[DeviceC-Vlan-interface11] quit
```

Verifying the configuration

Verify that PC A and PC B can ping each other successfully. This example uses PC A to ping PC B.

```
C:\>ping6 2001::2

Pinging 2001::2
from 1001::1 with 32 bytes of data:

Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms
Reply from 2001::2: bytes=32 time<1ms

Ping statistics for 2001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.13.2.2 255.255.255.0
#
interface Vlan-interface20
 ipv6 address 1001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ipv6 address 3001::1/64
 source 192.13.2.2
 destination 131.108.5.2
#
 ip route-static 131.108.5.2 255.255.255.0 192.13.2.1
#
 ipv6 route-static 2001:: 64 Tunnel 0
#
```

- Device B:

```
#
 service-loopback group 1 type tunnel
#
vlan 11
#
vlan 20
#
interface Vlan-interface11
 ip address 131.108.5.2 255.255.255.0
#
interface Vlan-interface20
 ipv6 address 2001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ipv6 address 3001::2/64
 source 131.108.5.2
 destination 192.13.2.2
#
ip route-static 192.13.2.2 255.255.255.0 131.108.5.1
```

```
#
ipv6 route-static 1001:: 64 Tunnel 0
#
```

- Device C:

```
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 192.13.2.1 255.255.255.0
#
interface Vlan-interface11
 ip address 131.108.5.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 11
#
```

Contents

Introduction

This document provides GRE with OSPF configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of GRE and OSPF.

Example: Configuring GRE with OSPF

Network configuration

As shown in Figure 1, Device A is the gateway of the headquarters. Device B and Device C are the gateways of Branch 1 and Branch 2, respectively. The gateways have obtained public IP addresses from an ISP and can communicate with one another. Configure GRE with OSPF to meet the following requirements:

- The headquarters and the branches communicate with one another through the GRE tunnels established between the headquarters and the branches.
- The gateways learn the routes reaching the destination networks through the tunnel interfaces.

Figure 1 Network diagram

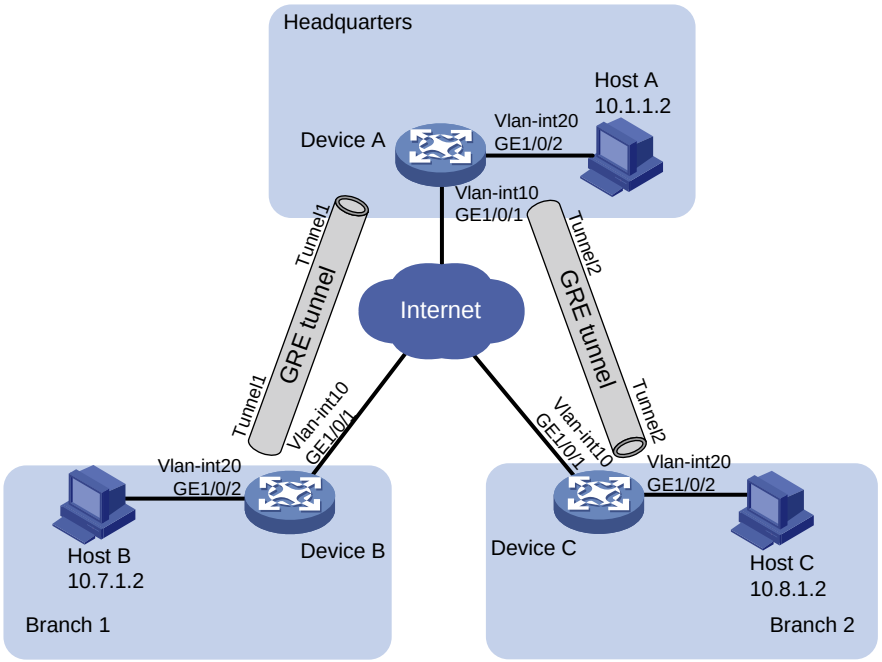


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int10	191.2.1.1/24	Device B	Vlan-int10	191.3.1.1/24
	Vlan-int20	10.1.1.1/24		Vlan-int20	10.7.1.1/24
	Tunnel1	10.5.1.1/24		Tunnel1	10.5.1.2/24
	Tunnel2	10.6.1.1/24			
Device C	Vlan-int10	191.4.1.1/24			
	Vlan-int20	10.8.1.1/24			
	Tunnel2	10.6.1.2/24			

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series	Not supported

Hardware	Software version
MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Before configuring GRE and OSPF, configure an IPv4 routing protocol on the gateways so that they can reach one another. (Details not shown.)

Configuring Device A

Configure VLAN-interface 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port GigabitEthernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-vlan-interface10] ip address 191.2.1.1 255.255.255.0
[DeviceA-vlan-interface10] quit
```

Configure other interfaces in the same way VLAN-interface 10 is configured. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceA] service-loopback group 1 type tunnel
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/3] quit
```

Create a tunnel interface **Tunnel 1**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceA] interface tunnel 1 mode gre
```

Configure an IP address for the tunnel interface **Tunnel 1**.

```
[DeviceA-Tunnel1] ip address 10.5.1.1 24
```

Configure the source interface of the tunnel interface **Tunnel 1** as VLAN-interface 10.

```
[DeviceA-Tunnel1] source vlan-interface 10
```

Configure the destination address of the tunnel interface **Tunnel 1** as the IP address of VLAN-interface 10 on Device B.

```
[DeviceA-Tunnel1] destination 191.3.1.1
[DeviceA-Tunnel1] quit
```

Create a tunnel interface **Tunnel 2**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceA] interface tunnel 2 mode gre
```

Configure an IP address for the tunnel interface **Tunnel 2**.

```
[DeviceA-Tunnel2] ip address 10.6.1.1 24
```

Configure the source interface of the tunnel interface **Tunnel 2** as VLAN-interface 10.

```
[DeviceA-Tunnel2] source vlan-interface 10
```

Configure the destination address of the tunnel interface **Tunnel 2** as the IP address of VLAN-interface 10 on Device C.

```
[DeviceA-Tunnel2] destination 191.4.1.1
[DeviceA-Tunnel2] quit
```

Configure the OSPF router ID as 10.6.1.1.

```
[DeviceA] router id  10.6.1.1
```

Enable OSPF process 1.

```
[DeviceA] ospf 1
```

Create OSPF area 0.

```
[DeviceA-ospf-1] area 0
```

Enable OSPF on interfaces whose primary IP addresses are on network 10.1.1.0/24, 10.5.1.0/24, or 10.6.1.0/24 in area 0.

```
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

Configuring Device B

Configure VLAN-interface 10.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port GigabitEthernet 1/0/1
[DeviceB-vlan10] quit
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 191.3.1.1 255.255.255.0
[DeviceB-vlan-interface10] quit
```

Configure other interfaces in the same way VLAN-interface 10 is configured. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceB] service-loopback group 1 type tunnel
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceB-GigabitEthernet1/0/3] quit
```

Create a tunnel interface **Tunnel 1**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceB] interface tunnel 1 mode gre
```

Configure an IP address for the tunnel interface **Tunnel 1**.

```
[DeviceB-Tunnel1] ip address 10.5.1.2 24
```

Configure the source interface of the tunnel interface **Tunnel 1** as VLAN-interface 10.

```
[DeviceB-Tunnel1] source Vlan-interface 10
```

Configure the destination address of the tunnel interface **Tunnel 1** as the IP address of VLAN-interface 10 on Device A.

```
[DeviceB-Tunnel1] destination 191.2.1.1
[DeviceB-Tunnel1] quit
```

Configure the OSPF router ID as 10.7.1.1.

```
[DeviceB] router id 10.7.1.1
```

Enable OSPF process 1.

```
[DeviceB] ospf 1
```

Create OSPF area 0.

```
[DeviceB-ospf-1] area 0
```

Enable OSPF on interfaces whose primary IP addresses are on network 10.7.1.0/24 or 10.5.1.0/24 in area 0.

```
[DeviceB-ospf-1-area-0.0.0.0] network 10.7.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
```

Configuring Device C

Configure VLAN-interface 10.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] port GigabitEthernet 1/0/1
[DeviceC-vlan10] quit
[DeviceC] interface Vlan-interface 10
[DeviceC-Vlan-interface10] ip address 191.4.1.1 255.255.255.0
[DeviceC-Vlan-interface10] quit
```

Configure other interfaces in the same way VLAN-interface 10 is configured. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/3 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceC] service-loopback group 1 type tunnel
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceC-GigabitEthernet1/0/3] quit
```

Create a tunnel interface **Tunnel 2**, and specify the tunnel mode as GRE/IPv4.

```
[DeviceC] interface tunnel 2 mode gre
```

Configure an IP address for the tunnel interface **Tunnel 2**.

```
[DeviceC-Tunnel2] ip address 10.6.1.2 24
```

Configure the source interface of the tunnel interface **Tunnel 2** as VLAN-interface 10.

```
[DeviceC-Tunnel2] source Vlan-interface 10
```

Configure the destination address of the tunnel interface **Tunnel 2** as the IP address of VLAN-interface 10 on Device A.

```
[DeviceC-Tunnel2] destination 191.2.1.1
[DeviceC-Tunnel2] quit
```

Configure the OSPF router ID as 10.8.1.1.

```
[DeviceC] router id 10.8.1.1
```

Enable OSPF process 1.

```
[DeviceC] ospf 1
```

Create OSPF area 0.

```
[DeviceC-ospf-1] area 0
```

Enable OSPF on interfaces whose primary IP addresses are on network 10.8.1.0/24 or 10.6.1.0/24 in area 0.

```
[DeviceC-ospf-1-area-0.0.0.0] network 10.8.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
```

Verifying the configuration

Verify that Host A can ping Host B successfully.

```
C:\> ping 10.7.1.2

Pinging 10.7.1.2 with 32 bytes of data:

Reply from 10.7.1.2: bytes=32 time=19ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253
Reply from 10.7.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 10.7.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Verify that Host A can ping Host C successfully.

```
C:\> ping 10.8.1.2

Pinging 10.8.1.2 with 32 bytes of data:

Reply from 10.8.1.2: bytes=32 time=18ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253
Reply from 10.8.1.2: bytes=32 time<1ms TTL=253

Ping statistics for 10.8.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Verify that Host B can ping Host C successfully.

```
C:\> ping 10.8.1.2

Pinging 10.8.1.2 with 32 bytes of data:

Reply from 10.8.1.2: bytes=32 time=20ms TTL=251
```

```
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251
Reply from 10.8.1.2: bytes=32 time<1ms TTL=251

Ping statistics for 10.8.1.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 191.2.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode gre
 source vlan-interface10
 destination 191.3.1.1
 ip address 10.5.1.1 255.255.255.0
#
interface Tunnel2 mode gre
 source vlan-interface10
 destination 191.4.1.1
```

```
 ip address 10.6.1.1 255.255.255.0
#
router id 10.6.1.1
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
#
```

- Device B

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 191.3.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.7.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode gre
 source Vlan-interface10
 destination 191.2.1.1
 ip address 10.5.1.2 255.255.255.0
#
router id 10.7.1.1
#
ospf 1
 area 0.0.0.0
  network 10.7.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
#
```

- Device C

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 191.4.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 10.8.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel2 mode gre
 source Vlan-interface10
 destination 191.2.1.1
 ip address 10.6.1.2 255.255.255.0
#
router id 10.8.1.1
#
ospf 1
 area 0.0.0.0
  network 10.8.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
#
```

Contents

Introduction

This document provides OSPF route filtering configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of OSPF route filtering.

Example: Configuring OSPF route filtering

Network configuration

As shown in Figure 1, the devices of an enterprise reside in OSPF and RIP domains.

Configure route redistribution between OSPF and RIP to interconnect the devices.

Configure route filtering on Device E, Device C, and Device D to meet the following requirements:

- The route destined for R&D department 2 is not redistributed to OSPF.
- Marketing department 1 cannot reach R&D department 1.
- R&D department 1 and the After-sale service department cannot reach Marketing department 2.

Figure 1 Network diagram

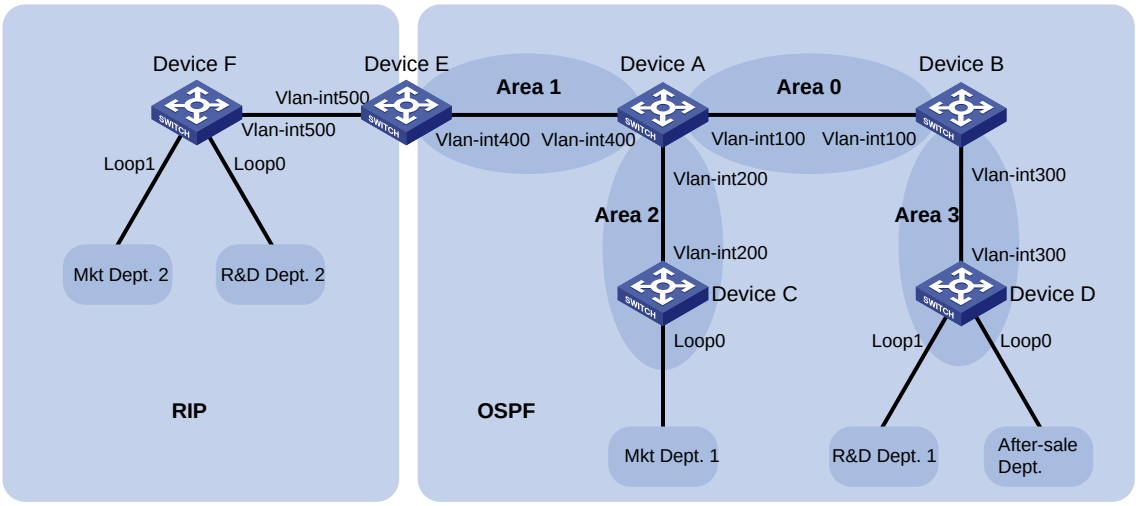


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int100	10.1.1.1/24	Device B	Vlan-int100	10.1.1.2/24
	Vlan-int200	10.2.1.1/24		Vlan-int300	10.3.1.1/24

Device	Interface	IP address	Device	Interface	IP address
	Vlan-int400	10.4.1.1/24			
Device C	Vlan-int200	10.2.1.2/24	Device D	Vlan-int300	10.3.1.2/24
	Loop0	192.168.3.1/24		Loop0	192.168.1.1/24
				Loop1	192.168.2.1/24
Device E	Vlan-int400	10.4.1.2/24	Device F	Vlan-int500	10.5.1.2/24
	Vlan-int500	10.5.1.1/24		Loop0	192.168.4.1/24
				Loop1	192.168.5.1/24

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure OSPF route filtering, follow these restrictions and guidelines:

- The **filter-policy export** command that filters redistributed routes takes effect only on an ASBR.
- OSPF filters routes calculated using received LSAs. It does not filter LSAs.
- IP communication is bidirectional. If a router filters out a route destined for Network A, the subnets attached to the router cannot reach Network A, and Network A cannot reach the subnets.
- When you configure route filtering by referencing an ACL, configure the **rule permit source any** item following multiple **rule deny source** items to allow unmatched routes to pass.

Procedures

Configuring IP addresses

Configure an IP address for VLAN-interface 100.

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ip address 10.1.1.1 24
```

Configure IP addresses for other interfaces in the same way VLAN-interface 100 is configured. (Details not shown.)

Configuring OSPF

Enable OSPF on Device A.

```
<DeviceA> system-view
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] area 2
[DeviceA-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.2] quit
[DeviceA-ospf-1] area 1
[DeviceA-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.1] quit
```

```
[DeviceA-ospf-1] quit
```

Enable OSPF on Device B.

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] area 3
[DeviceB-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.3] quit
[DeviceB-ospf-1] quit
```

Enable OSPF on Device C.

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 2
[DeviceC-ospf-1-area-0.0.0.2] network 10.2.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] network 192.168.3.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.2] quit
[DeviceC-ospf-1] quit
```

Enable OSPF on Device D.

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] area 3
[DeviceD-ospf-1-area-0.0.0.3] network 10.3.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] network 192.168.2.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.3] quit
[DeviceD-ospf-1] quit
```

Enable OSPF on Device E.

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 1
[DeviceE-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.1] quit
[DeviceE-ospf-1] quit
```

Configuring RIP

Enable RIP on Device E.

```
<DeviceE> system-view
[DeviceE] rip
[DeviceE-rip-1] version 2
[DeviceE-rip-1] undo summary
[DeviceE-rip-1] network 10.5.1.0 0.0.0.255
[DeviceE-rip-1] quit
```

Enable RIP on Device F.

```
<DeviceF> system-view
```

```
[DeviceF] rip
[DeviceF-rip-1] version 2
[DeviceF-rip-1] undo summary
[DeviceF-rip-1] network 10.5.1.0 0.0.0.255
[DeviceF-rip-1] network 192.168.4.0 0.0.0.255
[DeviceF-rip-1] network 192.168.4.0 0.0.0.255
[DeviceF-rip-1] quit
```

Configuring route redistribution

Configure Device E to redistribute OSPF and direct routes to RIP.

```
<DeviceE> system-view
[DeviceE] rip
[DeviceE-rip-1] import-route direct
[DeviceE-rip-1] import-route ospf
[DeviceE-rip-1] quit
```

Configure Device E to redistribute RIP and direct routes to OSPF.

```
[DeviceE] ospf
[DeviceE-ospf-1] import-route direct
[DeviceE-ospf-1] import-route rip
[DeviceE-ospf-1] quit
```

Verify that Device E has routes to all networks.

```
[DeviceE] display ip routing-table

Destinations : 24        Routes : 24

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.1.1.0/24        O_INTER 10  2           10.4.1.1        Vlan400
10.2.1.0/24        O_INTER 10  2           10.4.1.1        Vlan400
10.3.1.0/24        O_INTER 10  3           10.4.1.1        Vlan400
10.4.1.0/24        Direct  0   0           10.4.1.2        Vlan400
10.4.1.0/32        Direct  0   0           10.4.1.2        Vlan400
10.4.1.2/32        Direct  0   0           127.0.0.1       InLoop0
10.4.1.255/32      Direct  0   0           10.4.1.2        Vlan400
10.5.1.0/24        Direct  0   0           10.5.1.1        Vlan500
10.5.1.0/32        Direct  0   0           10.5.1.1        Vlan500
10.5.1.1/32        Direct  0   0           127.0.0.1       InLoop0
10.5.1.255/32      Direct  0   0           10.5.1.1        Vlan500
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.1/32     O_INTER 10  3           10.4.1.1        Vlan400
192.168.2.1/32     O_INTER 10  3           10.4.1.1        Vlan400
192.168.3.1/32     O_INTER 10  2           10.4.1.1        Vlan400
192.168.4.0/24     RIP     100 1           10.5.1.2        Vlan500
192.168.5.0/24     RIP     100 1           10.5.1.2        Vlan500
```

```
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Verify that other devices have routes to all networks. (Details not shown.)

Configuring OSPF route filtering

On Device C, configure IPv4 basic ACL 2000 to permit any subnet except 192.168.2.0/24.

```
<DeviceC> system-view
[DeviceC] acl basic 2000
[DeviceC-acl-ipv4-basic-2000] rule 0 deny source 192.168.2.0 0.0.0.255
[DeviceC-acl-ipv4-basic-2000] rule permit source any
[DeviceC-acl-ipv4-basic-2000] quit
```

On Device C, use ACL 2000 to filter received routes.

```
[DeviceC] ospf
[DeviceC-ospf-1] filter-policy 2000 import
[DeviceC-ospf-1] quit
```

On Device D, configure IPv4 basic ACL 2000 to permit any subnet except 192.168.5.0/24.

```
<DeviceD> system-view
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule 0 deny source 192.168.5.0 0.0.0.255
[DeviceD-acl-ipv4-basic-2000] rule permit source any
[DeviceD-acl-ipv4-basic-2000] quit
```

On Device D, use ACL 2000 to filter received routes.

```
[DeviceD] ospf
[DeviceD-ospf-1] filter-policy 2000 import
[DeviceD-ospf-1] quit
```

On Device E, configure IPv4 basic ACL 2000 to permit any subnet except 192.168.4.0/24.

```
<DeviceE> system-view
[DeviceE] acl basic 2000
[DeviceE-acl-ipv4-basic-2000] rule 0 deny source 192.168.4.0 0.0.0.255
[DeviceE-acl-ipv4-basic-2000] rule permit source any
[DeviceE-acl-ipv4-basic-2000] quit
```

On Device E, use ACL 2000 to filter routes redistributed from RIP.

```
[DeviceE] ospf
[DeviceE-ospf-1] filter-policy 2000 export rip 1
[DeviceE-ospf-1] quit
```

Verifying the configuration

Verify that Device C does not have a route to 192.168.2.0/24.

```
[DeviceC] display ip routing-table

Destinations : 22        Routes : 22

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
```

```
10.1.1.0/24        O_INTER 10  2           10.2.1.1        Vlan200
10.2.1.0/24        Direct  0   0           10.2.1.2        Vlan200
10.2.1.0/32        Direct  0   0           10.2.1.2        Vlan200
10.2.1.2/32        Direct  0   0           127.0.0.1       InLoop0
10.2.1.255/32      Direct  0   0           10.2.1.2        Vlan200
10.3.1.0/24        O_INTER 10  3           10.2.1.1        Vlan200
10.4.1.0/24        O_INTER 10  2           10.2.1.1        Vlan200
10.5.1.0/24        O_ASE2  150 1           10.2.1.1        Vlan200
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.1/32     O_INTER 10  3           10.2.1.1        Vlan200
192.168.3.0/24     Direct  0   0           192.168.3.1     Loop0
192.168.3.0/32     Direct  0   0           192.168.3.1     Loop0
192.168.3.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.3.255/32   Direct  0   0           192.168.3.1     Loop0
192.168.5.0/24     O_ASE2  150 1           10.2.1.1        Vlan200
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Verify that Marketing department 1 cannot reach R&D department 1.

```
[DeviceC] ping -a 192.168.3.1 192.168.2.1
Ping 192.168.2.1 (192.168.2.1) from 192.168.3.1: 56 data bytes, press CTRL+C to
break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Verify that Device D does not have a route to 192.168.5.0/24.

```
[DeviceD] display ip routing-table

Destinations : 25        Routes : 25

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.1.1.0/24        O_INTER 10  2           10.3.1.1        Vlan300
10.2.1.0/24        O_INTER 10  3           10.3.1.1        Vlan300
10.3.1.0/24        Direct  0   0           10.3.1.2        Vlan300
10.3.1.0/32        Direct  0   0           10.3.1.2        Vlan300
10.3.1.2/32        Direct  0   0           127.0.0.1       InLoop0
10.3.1.255/32      Direct  0   0           10.3.1.2        Vlan300
10.4.1.0/24        O_INTER 10  3           10.3.1.1        Vlan300
10.5.1.0/24        O_ASE2  150 1           10.3.1.1        Vlan300
```

```
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.1.0/24     Direct  0   0           192.168.1.1     Loop0
192.168.1.0/32     Direct  0   0           192.168.1.1     Loop0
192.168.1.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32   Direct  0   0           192.168.1.1     Loop0
192.168.2.0/24     Direct  0   0           192.168.2.1     Loop1
192.168.2.0/32     Direct  0   0           192.168.2.1     Loop1
192.168.2.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.2.255/32   Direct  0   0           192.168.2.1     Loop1
192.168.3.1/32     O_INTER 10  3           10.3.1.1        Vlan300
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Verify that the After-sale service department cannot reach Marketing department 2.

```
[DeviceD] ping -a 192.168.1.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.1.1: 56 data bytes, press CTRL+C to
break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.5.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Verify that R&D department 1 cannot reach Marketing department 2.

```
[DeviceD] ping -a 192.168.2.1 192.168.5.1
Ping 192.168.5.1 (192.168.5.1) from 192.168.2.1: 56 data bytes, press CTRL+C to
break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 192.168.5.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

The output on Device C and Device D shows that Device E has filtered out the route destined for R&D development 2.

Configuration files

- Device A:

  ```
  #
  ```

```
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.1
network 10.4.1.0 0.0.0.255
area 0.0.0.2
  network 10.2.1.0 0.0.0.255
#
vlan 100
#
vlan 200
#
vlan 400
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.4.1.1 255.255.255.0
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.3.1.1 255.255.255.0
#
```

- Device C:

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.2
  network 10.2.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
```

```
#
vlan 200
#
interface LoopBack0
 ip address 192.168.3.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.2.0 0.0.0.255
rule 5 permit
#
```

- Device D:

```
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
vlan 300
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface300
 ip address 10.3.1.2 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.5.0 0.0.0.255
rule 5 permit
#
```

- Device E:

```
#
ospf 1
 import-route direct
 import-route rip 1
 filter-policy 2000 export rip 1
 area 0.0.0.1
  network 10.4.1.0 0.0.0.255
#
rip 1
 undo summary
```

```
 version 2
 network 10.5.1.0 0.0.0.255
 import-route direct
 import-route ospf 1
#
vlan 400
#
vlan 500
#
interface Vlan-interface400
 ip address 10.4.1.2 255.255.255.0
#
interface Vlan-interface500
 ip address 10.5.1.1 255.255.255.0
#
acl basic 2000
 rule 0 deny source 192.168.4.0 0.0.0.255
rule 5 permit
#
```

- Device F:

```
#
rip 1
 undo summary
 version 2
 network 10.5.1.0 0.0.0.255
 network 192.168.4.0
 network 192.168.5.0
#
vlan 500
#
interface LoopBack0
 ip address 192.168.4.1 255.255.255.0
#
interface LoopBack1
 ip address 192.168.5.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.5.1.2 255.255.255.0
#
```

Contents

Introduction

This document provides IS-IS configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IS-IS.

Example: Configuring IS-IS

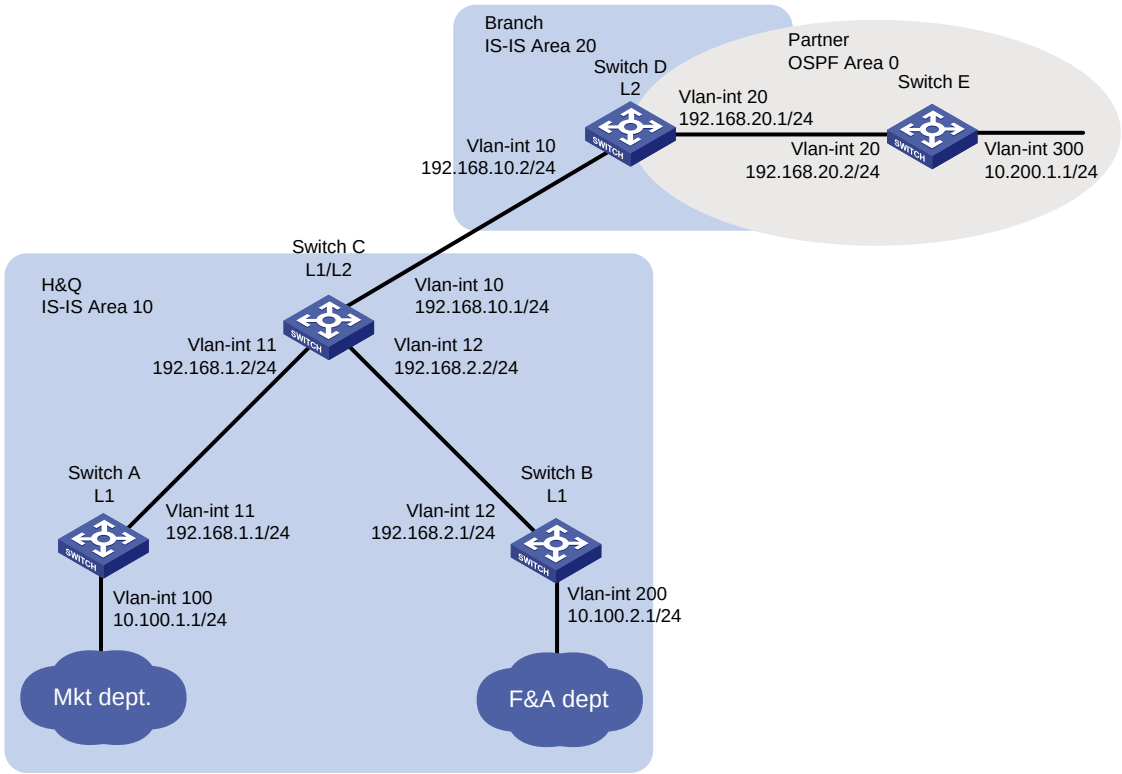
Network configuration

As shown in Figure 1, the company's headquarters and the branch run IS-IS. The partner runs OSPF.

Configure the switches to meet the following requirements:

- The marketing department can reach the finance department, the branch, and the partner.
- The finance department and the branch cannot reach each other, and the branch does not have a route to the finance department.
- When the IS-IS process on Switch C restarts, the communication is not interrupted.

Figure 1 Network diagram



Analysis

To allow communication between the marketing department and the finance department, configure Switch A and Switch B in Area 10 as Level-1 routers.

To allow communication between the marketing department and the partner, configure route redistribution between IS-IS and OSPF on Switch D.

To ensure that the branch does not have a route to the finance department, configure Switch C to use a prefix list to advertise only network 10.100.1.0/24 to Level-2.

To ensure that the communication is not interrupted when the IS-IS process on Switch C restarts, enable IS-IS Graceful Restart (GR) on Switch C.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported

WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

To avoid blackhole routes, do not change the network topology during the IS-IS GR process.

Procedures

Configuring Switch A

Configure an IP address for VLAN-interface 11.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 192.168.1.1 24
[SwitchA-Vlan-interface11] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IS-IS.

```
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.1921.6800.1001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 11
[SwitchA–Vlan-interface11] isis enable 1
[SwitchA–Vlan-interface11] quit
[SwitchA] interface vlan-interface 100
[SwitchA–Vlan-interface100] isis enable 1
[SwitchA–Vlan-interface100] quit
```

Configuring Switch B

Configure an IP address for VLAN-interface 12.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 12
[SwitchB-Vlan-interface12] ip address 192.168.2.1 24
[SwitchB-Vlan-interface12] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IS-IS.

```
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
```

```
[SwitchB-isis-1] network-entity 10.1921.6800.2001.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 12
[SwitchB–Vlan-interface12] isis enable 1
[SwitchB–Vlan-interface12] quit
[SwitchB] interface vlan-interface 200
[SwitchB–Vlan-interface 200] isis enable 1
[SwitchB–Vlan-interface 200] quit
```

Configuring Switch C

Configure an IP address for VLAN-interface 11.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 11
[SwitchC-Vlan-interface11] ip address 192.168.1.2 24
[SwitchC-Vlan-interface11] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IS-IS.

```
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.1921.6801.0001.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 10
[SwitchC–Vlan-interface10] isis enable 1
[SwitchC–Vlan-interface10] quit
[SwitchC] interface vlan-interface 11
[SwitchC–Vlan-interface11] isis enable 1
[SwitchC–Vlan-interface11] quit
[SwitchC] interface vlan-interface 12
[SwitchC–Vlan-interface12] isis enable 1
[SwitchC–Vlan-interface12] quit
```

Configure route leaking from Level-1 to Level-2, and use prefix list 1 to advertise only network 10.100.1.0/24 to Level-2.

```
[SwitchC] ip prefix-list 1 permit 10.100.1.0 24
[SwitchC] isis 1
[SwitchC-isis-1] address-family ipv4
[SwitchC-isis-1-ipv4] import-route isis level-1 into level-2 filter-policy prefix-list
1
[SwitchC-isis-1-ipv4] quit
```

Enable IS-IS GR.

```
[SwitchC-isis-1] graceful-restart
[SwitchC-isis-1] quit
```

Configuring Switch D

Configure an IP address for VLAN-interface 10.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 10
[SwitchD-Vlan-interface10] ip address 192.168.10.2 24
```

```
[SwitchD-Vlan-interface10] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IS-IS.

```
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 10.1921.6802.0001.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 10
[SwitchD–Vlan-interface10] isis enable 1
[SwitchD–Vlan-interface10] quit
[SwitchD] interface vlan-interface 20
[SwitchD–Vlan-interface20] isis enable 1
[SwitchD–Vlan-interface20] quit
```

Configure OSPF.

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Redistribute OSPF and direct routes into IS-IS

```
[SwitchD] isis 1
[SwitchD-isis-1] address-family ipv4
[SwitchD-isis-1-ipv4] import-route ospf
[SwitchD-isis-1-ipv4] import-route direct
[SwitchD-isis-1-ipv4] quit
[SwitchD-isis-1] quit
```

Redistribute IS-IS and direct routes into OSPF.

```
[SwitchD] ospf 1
[SwitchD-ospf-1] import-route isis 1
[SwitchD-ospf-1] import-route direct
```

Configuring Switch E

Configure an IP address for VLAN-interface 20.

```
<SwitchE> system-view
[SwitchE] interface vlan-interface20
[SwitchE-Vlan-interface12] ip address 192.168.20.2 24
[SwitchE-Vlan-interface12] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure OSPF.

```
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.200.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

Verifying the configuration

Verify that the branch can reach the marketing department, but cannot reach the finance department.

```
[SwitchD] display isis route
                        Route information for IS-IS(1)
                        ------------------------------
                        Level-2 IPv4 Forwarding Table
                        ------------------------------
 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    Vlan10          Direct          D/L/-
 192.168.1.0/24       20         NULL    Vlan10          192.168.10.1    R/-/-
 10.100.1.0/24        30         NULL    Vlan10          192.168.10.1    R/-/-
 192.168.2.0/24       20         NULL    Vlan10          192.168.10.1    R/-/-
      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Verify that the marketing department can communicate with the partner.

- Display the IS-IS routing table on Switch C.

```
[SwitchC] display isis route
                        Route information for IS-IS(1)
                        ------------------------------
                        Level-1 IPv4 Forwarding Table
                        ------------------------------
 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    Vlan10          Direct          D/L/-
 192.168.1.0/24       10         NULL    Vlan11          Direct          D/L/-
 10.100.1.0/24        20         NULL    Vlan11          192.168.1.1     R/L/-
 10.100.2.0/24        20         NULL    Vlan12          192.168.2.1     R/-/-
 192.168.2.0/24       10         NULL    Vlan12          Direct          D/L/-
      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
                        Level-2 IPv4 Forwarding Table
                        ------------------------------
 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 192.168.10.0/24      10         NULL    Vlan10          Direct          D/L/-
 10.200.1.0/24        10         0       Vlan10          192.168.10.2    R/-/-
 192.168.20.0/24      10         0       Vlan10          192.168.10.2    R/-/-
 192.168.1.0/24       10         NULL    Vlan11          Direct          D/L/-
 192.168.2.0/24       10         NULL    Vlan12          Direct          D/L/-
      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

- Ping 10.200.1.1 from Switch A.

```
[SwitchA] ping 10.200.1.1
Ping 10.200.1.1 (10.200.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 10.200.1.1: icmp_seq=0 ttl=254 time=1.862 ms
56 bytes from 10.200.1.1: icmp_seq=1 ttl=254 time=2.969 ms
56 bytes from 10.200.1.1: icmp_seq=2 ttl=254 time=1.402 ms
```

```
56 bytes from 10.200.1.1: icmp_seq=3 ttl=254 time=1.324 ms
56 bytes from 10.200.1.1: icmp_seq=4 ttl=254 time=1.510 ms
--- Ping statistics for 10.200.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.324/1.813/2.969/0.606 ms
```

Verify that the communication is not interrupted when the IS-IS process restarts.

- Ping Switch B from Switch A.

```
[SwitchA] ping -c 10000 10.100.2.1
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL+C to break
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
…
```

- Restart the IS-IS process on Switch C.

```
[SwitchC] reset isis all graceful-restart
Reset IS-IS process? [Y/N] :y
```

Ping Switch B from Switch A.

```
[SwitchA] ping -c 10000 10.100.2.1
Ping 10.100.2.1 (10.100.2.1): 56 data bytes, press CTRL+C to break
56 bytes from 10.100.2.1: icmp_seq=0 ttl=254 time=1.185 ms
56 bytes from 10.100.2.1: icmp_seq=1 ttl=254 time=1.087 ms
56 bytes from 13.13.13.3: icmp_seq=2 ttl=254 time=1.672 ms
56 bytes from 13.13.13.3: icmp_seq=3 ttl=254 time=1.751 ms
56 bytes from 13.13.13.3: icmp_seq=4 ttl=254 time=1.816 ms
56 bytes from 13.13.13.3: icmp_seq=5 ttl=254 time=1.814 ms
```

Check the IS-IS GR state on Switch C.

```
[SwitchC] display isis graceful-restart status
                        Restart information for IS-IS(1)
                        --------------------------------
Restart status: COMPLETE
Restart phase: Finish
Restart t1: 3, count 10; Restart t2: 60; Restart t3: 300
SA Bit: supported
                          Level-1 restart information
                          ---------------------------
Total number of interfaces: 3
Number of waiting LSPs: 0
                          Level-2 restart information
                          ---------------------------
Total number of interfaces: 3
Number of waiting LSPs: 0
```

Configuration files

- Switch A:

```
#
isis 1
 is-level level-1
```

```
 network-entity 10.1921.6800.1001.00
#
vlan 11
#
vlan 100
#
interface Vlan-interface11
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
interface Vlan-interface100
 ip address 10.100.1.1 255.255.255.0
 isis enable 1
#
```

- Switch B:

```
#
isis 1
 is-level level-1
 network-entity 10.1921.6800.2001.00
#
vlan 12
#
vlan 200
#
interface Vlan-interface12
 ip address 192.168.2.1 255.255.255.0
 isis enable 1
#
interface Vlan-interface200
 ip address 10.100.2.1 255.255.255.0
 isis enable 1
#
```

- Switch C:

```
#
isis 1
 graceful-restart
 network-entity 10.1921.6801.0001.00
 #
 address-family ipv4 unicast
  import-route isis level-1 into level-2 filter-policy prefix-list 1
#
vlan 11 to 13
#
interface Vlan-interface11
 ip address 192.168.1.2 255.255.255.0
 isis enable 1
#
interface Vlan-interface12
```

```
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
interface Vlan-interface13
 ip address 192.168.10.1 255.255.255.0
 isis enable 1
#
 ip prefix-list 1 index 10 permit 10.100.1.0 24
#
```

- Switch D:

```
#
isis 1
 is-level level-2
 network-entity 20.1921.6802.0001.00
#
 address-family ipv4 unicast
  import-route direct
  import-route ospf 1
#
ospf 1
 import-route direct
 import-route isis 1
 area 0.0.0.0
  network 192.168.20.0 0.0.0.255
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.10.2 255.255.255.0
 isis enable 1
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
```

- Switch E:

```
#
ospf 1
 area 0.0.0.0
  network 10.200.1.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
vlan 20
#
vlan 300
#
interface Vlan-interface20
```

```
 ip address 192.168.20.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.200.1.1 255.255.255.0
#
```

Contents

Introduction

This document provides BGP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

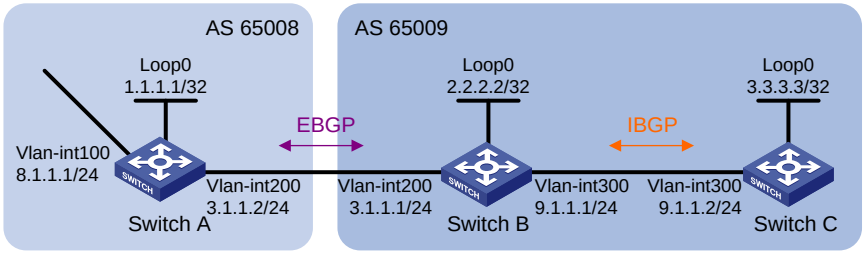
This document assumes that you have basic knowledge of BGP.

Example: Configuring basic BGP

Network configuration

As shown in Figure 1, all switches run BGP. Run EBGP between Switch A and Switch B, and run IBGP between Switch B and Switch C so that Switch C can access the network 8.1.1.0/24 connected to Switch A.

Figure 1 Network diagram



Analysis

To enable Switch B to communicate with Switch C through loopback interfaces, enable OSPF in AS 65009.

By default, BGP does not advertise local networks. To enable Switch C to access the network 8.1.1.0/24 connected directly to Switch A, perform the following tasks:

- Inject network 8.1.1.0/24 to the BGP routing table of Switch A.
- Inject networks 3.1.1.0/24 and 9.1.1.0/24 to the BGP routing table of Switch B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure basic BGP, follow these restrictions and guidelines:

- Use loopback interfaces to establish IBGP connections to prevent route flapping caused by port state changes.

- Loopback interfaces are virtual interfaces. Use the **peer connect-interface** command to specify the loopback interface as the source interface for establishing BGP connections.
- The EBGP peers, Switch A and Switch B, are located in different ASs. Typically, their loopback interfaces are not reachable to each other, so the switches use directly connected interfaces to establish EBGP sessions.

Procedures

Configuring IP addresses for interfaces

Configure an IP address for VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 8.1.1.1 24
```

Configure IP addresses for other interfaces in the same way that VLAN-interface 100 is configured. (Details not shown.)

Configuring IBGP

Configuring Switch B

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp-default] router-id 2.2.2.2
[SwitchB-bgp-default] peer 3.3.3.3 as-number 65009
[SwitchB-bgp-default] peer 3.3.3.3 connect-interface Loopback 0
[SwitchB-bgp-default] address-family ipv4 unicast
[SwitchB-bgp-default-ipv4] peer 3.3.3.3 enable
[SwitchB-bgp-default-ipv4] quit
[SwitchB-bgp-default] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp-default] router-id 3.3.3.3
[SwitchC-bgp-default] peer 2.2.2.2 as-number 65009
[SwitchC-bgp-default] peer 2.2.2.2 connect-interface Loopback 0
[SwitchC-bgp-default] address-family ipv4 unicast
[SwitchC-bgp-default-ipv4] peer 2.2.2.2 enable
[SwitchC-bgp-default-ipv4] quit
[SwitchC-bgp-default] quit
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
```

```
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Display BGP peer information on Switch C.

```
[SwitchC] display bgp peer ipv4
 BGP local router ID : 3.3.3.3
 Local AS number : 65009
 Total number of peers : 1                 Peers in established state : 1

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  2.2.2.2              65009        2        2    0       0 00:00:13 Established
```

The output shows that Switch C has established an IBGP peer relationship with Switch B.

Configuring EBGP

Configuring Switch A

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp-default] router-id 1.1.1.1
[SwitchA-bgp-default] peer 3.1.1.1 as-number 65009
[SwitchA-bgp-default] address-family ipv4 unicast
[SwitchA-bgp-default-ipv4] peer 3.1.1.1 enable
[SwitchA-bgp-default-ipv4] network 8.1.1.0 24
[SwitchA-bgp-default-ipv4] quit
[SwitchA-bgp-default] quit
```

Configuring Switch B

```
[SwitchB] bgp 65009
[SwitchB-bgp-default] peer 3.1.1.2 as-number 65008
[SwitchB-bgp-default] address-family ipv4 unicast
[SwitchB-bgp-default-ipv4] peer 3.1.1.2 enable
[SwitchB-bgp-default-ipv4] quit
[SwitchB-bgp-default] quit
```

Display BGP peer information on Switch B.

```
[SwitchB] display bgp peer ipv4
 BGP local router ID : 2.2.2.2
 Local AS number : 65009
 Total number of peers : 2                 Peers in established state : 2

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  3.3.3.3              65009        4        4    0       0 00:02:49 Established
```

```
  3.1.1.2              65008        2        2    0       0 00:00:05 Established
```

The output shows that Switch B has established an IBGP peer relationship with Switch C and an EBGP peer relationship with Switch A.

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing-table ipv4
 Total number of routes: 1
 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  8.1.1.0/24         8.1.1.1         0                     32768   i
```

Display the BGP routing table on Switch B.

```
[SwitchB] display bgp routing-table ipv4
 Total number of routes: 1
 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >e 8.1.1.0/24         3.1.1.2         0                     0       65008i
```

Display the BGP routing table on Switch C.

```
[SwitchC] display bgp routing-table ipv4
 Total number of routes: 1
 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
   i 8.1.1.0/24         3.1.1.2         0          100        0       65008i
```

The outputs show that Switch A has learned no route to AS 65009, and Switch C has learned network 8.1.1.0, but the next hop 3.1.1.2 is unreachable. As a result, the route is invalid.

Configuring BGP to redistribute direct routes on Switch B

Configure Switch B.

```
[SwitchB] bgp 65009
[SwitchB-bgp-default] address-family ipv4 unicast
[SwitchB-bgp-default-ipv4] network 3.1.1.0 24
[SwitchB-bgp-default-ipv4] network 9.1.1.0 24
[SwitchB-bgp-default-ipv4] quit
[SwitchB-bgp-default] quit
```

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing-table ipv4
```

```
 Total number of routes: 3
 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >e 3.1.1.0/24         3.1.1.1         0                     0       65009?
* >  8.1.1.0/24         8.1.1.1         0                     32768   i
* >e 9.1.1.0/24         3.1.1.1         0                     0       65009i
```

The output shows that route 9.1.1.0/24 has been added in Switch A's routing table.

Display the BGP routing table on Switch C.

```
[SwitchC] display bgp routing-table ipv4
 Total number of routes: 3
 BGP local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >i 3.1.1.0/24         2.2.2.2         0          100        0       ?
* >i 8.1.1.0/24         3.1.1.2         0          100        0       65008i
* >i 9.1.1.0/24         2.2.2.2         0          100        0       i
```

The output shows that the route 8.1.1.0 becomes valid with the next hop as Switch A.

Verifying the configuration

Verify that Switch C can ping 8.1.1.1.

```
[SwitchC] ping 8.1.1.1
Ping 8.1.1.1 (8.1.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms
--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.800/10.000/2.638 ms
```

Configuration files

- Switch A:

  ```
  #
  vlan 100
  #
  vlan 200
  #
  ```

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface100
 ip address 8.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
router-id 1.1.1.1
peer 3.1.1.1 as-number 65009
#
address-family ipv4 unicast
network 8.1.1.0 255.255.255.0
peer 3.1.1.1 enable
#
```

- Switch B:

```
#
vlan 200
#
vlan 300
#
interface Loopback0
ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface200
ip address 3.1.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 9.1.1.1 255.255.255.0
#
bgp 65009
router-id 2.2.2.2
peer 3.1.1.2 as-number 65008
peer 3.3.3.3 as-number 65009
peer 3.3.3.3 connect-interface Loopback0
#
address-family ipv4 unicast
network 3.1.1.0 255.255.255.0
network 9.1.1.0 255.255.255.0
peer 3.1.1.2 enable
peer 3.3.3.3 enable
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
```

```
#
```

- Switch C:

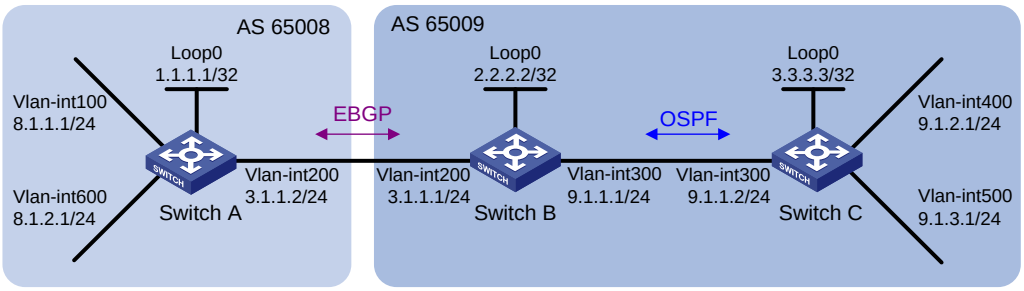
```
#
vlan 300
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface300
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
peer 2.2.2.2 as-number 65009
peer 2.2.2.2 connect-interface Loopback0
#
address-family ipv4 unicast
peer 2.2.2.2 enable
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

Examples: Configuring BGP and IGP route redistribution

Network configuration

As shown in Figure 2, all devices of company A belong to AS 65008 and all devices of company B belong to AS 65009. Run EBGP between Switch A and Switch B, and run OSPF between Switch B and Switch C to allow communication only between networks 9.1.2.0/24 and 8.1.1.0/24.

Figure 2 Network diagram



Analysis

To enable Switch B to communicate with Switch C through loopback interfaces, enable OSPF in AS 65009.

To enable Switch A to obtain the route to 9.1.2.0/24, configure BGP to redistribute routes from OSPF on Switch B. To enable Switch C to obtain the route to 8.1.1.0/24, configure OSPF to redistribute routes from BGP on Switch B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch	Not supported

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure BGP and IGP route redistribution, follow these restrictions and guidelines:

- Use loopback interfaces to establish IBGP connections to prevent route flapping caused by port state changes.
- Loopback interfaces are virtual interfaces. Use the **peer connect-interface** command to specify the loopback interface as the source interface for establishing BGP connections.
- The EBGP peers, Switch A and Switch B, are located in different ASs. Typically, their loopback interfaces are not reachable to each other, so the switches directly connected interfaces to establish EBGP sessions.

Procedures

Configuring IP addresses for interfaces

Configure an IP address for VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 8.1.1.1 24
```

Configure IP addresses for other interfaces in the same way that VLAN-interface 100 is configured. (Details not shown.)

Enabling OSPF

Enable OSPF in AS 65009.

Configuring Switch B

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 9.1.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
```

```
[SwitchC-ospf-1] quit
```

Configuring EBGP connection

Configure the EBGP connection and inject network 8.1.1.0/24 to the BGP routing table of Switch A.

Configuring Switch A

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp-default] router-id 1.1.1.1
[SwitchA-bgp-default] peer 3.1.1.1 as-number 65009
[SwitchA-bgp-default] address-family ipv4 unicast
[SwitchA-bgp-default-ipv4] peer 3.1.1.1 enable
[SwitchA-bgp-default-ipv4] network 8.1.1.0 24
[SwitchA-bgp-default-ipv4] quit
[SwitchA-bgp-default] quit
```

Configuring Switch B

```
[SwitchB] bgp 65009
[SwitchB-bgp-default] router-id 2.2.2.2
[SwitchB-bgp-default] peer 3.1.1.2 as-number 65008
[SwitchB-bgp-default] address-family ipv4 unicast
[SwitchB-bgp-default-ipv4] peer 3.1.1.2 enable
```

Configuring BGP and IGP route redistribution

Configure route redistribution between BGP and OSPF on Switch B.

```
[SwitchB-bgp-default-ipv4] import-route ospf 1
[SwitchB-bgp-default-ipv4] quit
[SwitchB-bgp-default] quit
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

Display the BGP routing table on Switch A.

```
[SwitchA] display bgp routing-table ipv4
 Total number of routes: 3
 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  8.1.1.0/24         8.1.1.1         0                     32768   i
* >e 9.1.2.0/24         3.1.1.1         1                     0       65009?
```

The output shows that Switch A has obtained the route to 9.1.2.0/24.

Display the OSPF routing table on Switch C.

```
[SwitchC] display ospf routing
          OSPF Process 1 with Router ID 3.3.3.3
```

```
                  Routing Table

               Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 9.1.1.0/24         1        Transit 9.1.1.2         3.3.3.3         0.0.0.0
9.1.2.0/24         1        Stub    9.1.2.1         192.168.0.63    0.0.0.0
 2.2.2.2/32         1        Stub    9.1.1.1         2.2.2.2         0.0.0.0
 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 8.1.1.0/24         1        Type2   1           9.1.1.1         2.2.2.2
 Total nets: 3
 Intra area: 2  Inter area: 0  ASE: 1  NSSA: 0
```

The output shows that Switch C has obtained the route to 8.1.1.0/24.

Verifying the configuration

Ping 9.1.2.1 from 8.1.1.1 on Switch A. The ping operation succeeds.

```
[SwitchA] ping -a 8.1.1.1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.1.1: 56 data bytes, press CTRL+C to break
56 bytes from 9.1.2.1: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 9.1.2.1: icmp_seq=1 ttl=254 time=12.000 ms
56 bytes from 9.1.2.1: icmp_seq=2 ttl=254 time=2.000 ms
56 bytes from 9.1.2.1: icmp_seq=3 ttl=254 time=7.000 ms
56 bytes from 9.1.2.1: icmp_seq=4 ttl=254 time=9.000 ms
--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/8.000/12.000/3.406 ms
```

Ping 8.1.1.1 from 9.1.2.1 on Switch C. The ping operation succeeds.

```
[SwitchC] ping -a 9.1.2.1 8.1.1.1
Ping 8.1.1.1 (8.1.1.1) from 9.1.2.1: 56 data bytes, press CTRL+C to break
56 bytes from 8.1.1.1: icmp_seq=0 ttl=254 time=9.000 ms
56 bytes from 8.1.1.1: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 8.1.1.1: icmp_seq=2 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 8.1.1.1: icmp_seq=4 ttl=254 time=3.000 ms
--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.400/9.000/2.332 ms
```

Ping 9.1.2.1 and 9.1.3.1 from 8.1.2.1 on Switch A. The ping operations fail.

```
[SwitchA] ping –a 8.1.2.1 9.1.2.1
Ping 9.1.2.1 (9.1.2.1) from 8.1.2.1: 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
```

```
Request time out
--- Ping statistics for 9.1.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
[SwitchA] ping –a 8.1.2.1 9.1.3.1
Ping 9.1.3.1 (9.1.3.1) from 8.1.2.1: 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- Ping statistics for 9.1.3.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Ping 8.1.1.1 and 8.1.2.1 from 9.1.3.1 on Switch C. The ping operations fail.

```
[SwitchC] ping –a 9.1.3.1 8.1.1.1
Ping 8.1.1.1 (8.1.1.1) from 9.1.3.1: 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- Ping statistics for 8.1.1.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
[SwitchC] ping –a 9.1.3.1 8.1.2.1
Ping 8.1.2.1 (8.1.2.1) from 9.1.3.1: 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- Ping statistics for 8.1.2.1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
vlan 600
#
interface Loopback0
ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface100
 ip address 8.1.1.1 255.255.255.0
#
```

```
interface Vlan-interface200
ip address 3.1.1.2 255.255.255.0
#
interface Vlan-interface600
ip address 8.1.2.1 255.255.255.0
#
bgp 65008
router-id 1.1.1.1
peer 3.1.1.1 as-number 65009
#
address-family ipv4 unicast
network 8.1.1.0 255.255.255.0
peer 3.1.1.1 enable
#
```

- Switch B:

```
#
vlan 200
#
vlan 300
#
vlan 500
#
interface Loopback0
ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface200
ip address 3.1.1.1 255.255.255.0
#
interface Vlan-interface300
ip address 9.1.1.1 255.255.255.0
#
bgp 65009
router-id 2.2.2.2
peer 3.1.1.2 as-number 65008
#
address-family ipv4 unicast
import-route ospf 1
peer 3.1.1.2 enable
#
ospf 1
import-route bgp
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 9.1.1.0 0.0.0.255
#
```

- Switch C:

```
#
vlan 300
```

```
#
vlan 400
#
interface Loopback0
ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface300
ip address 9.1.1.2 255.255.255.0
#
interface Vlan-interface400
ip address 9.1.2.1 255.255.255.0
#
interface Vlan-interface500
ip address 9.1.3.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 9.1.1.0 0.0.0.255
network 9.1.2.0 0.0.0.255
#
```

Contents

Introduction

This document provides PBR configuration examples.

PBR uses a user-defined policy to route packets based on fields such as the source address, destination address, IP precedence, and protocol. PBR takes precedence over destination-based routing.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of PBR.

Configuration restrictions and guidelines

When you configure the action of forwarding traffic to a next hop, do not specify the following addresses:

- An IPv6 address in an IPv4 ACL rule.
- An IPv4 address in an IPv6 ACL rule.

Example: Configuring PBR

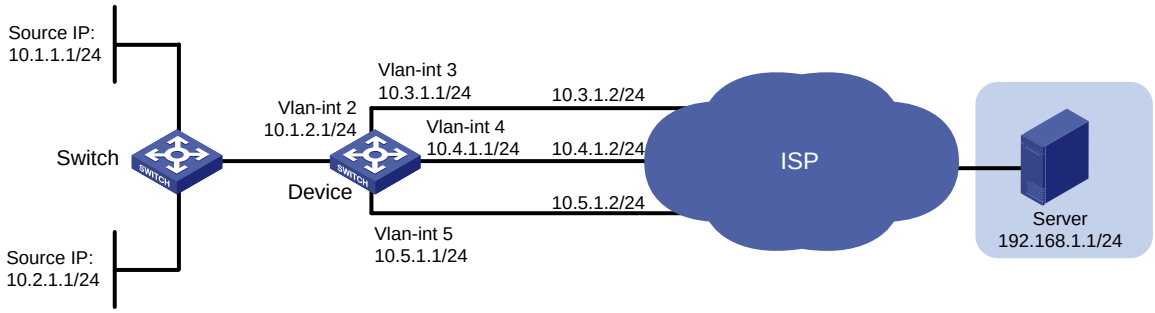
Network configuration

As shown in Figure 1, on Device, all packets destined for Server are forwarded to the next hop 10.4.1.2 by default.

Configure PBR to meet the following requirements:

- Packets with source IPv4 address 10.2.1.1 received on VLAN-interface 2 are forwarded to the next hop 10.5.1.2.
- HTTP packets with source IPv4 addresses other than 10.2.1.1 received on VLAN-interface 2 are forwarded to the next hop 10.3.1.2.

Figure 1 Network diagram



Analysis

To forward the two types of packets to different next hops, you must perform the following tasks:

- Configure two ACLs to classify the two types of packets.
- Configure two policy nodes to forward the packets to the specified next hops.

To ensure that packets with source address 10.2.1.1 are forwarded to the next hop 10.5.1.2, assign a node a smaller node ID to match the packets.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx

IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6658P01 and later

Procedures

Configure an IPv4 address for VLAN-interface 2.

```
<Device> system-view
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 10.1.2.1 255.255.255.0
[Device-Vlan-interface2] quit
```

Configure IPv4 addresses for other interfaces in the same way VLAN-interface 2 is configured. (Details not shown.)

Configure three static routes and configure 10.4.1.2 as the default next hop.

```
[Device] ip route-static 192.168.1.0 24 10.3.1.2
[Device] ip route-static 192.168.1.0 24 10.4.1.2 preference 40
[Device] ip route-static 192.168.1.0 24 10.5.1.2
```

Create ACL 3005 to match packets with source address 10.2.1.1.

```
[Device] acl advanced 3005
[Device-acl-ipv4-adv-3005] rule 0 permit ip source 10.2.1.1 0
[Device-acl-ipv4-adv-3005] quit
```

Create ACL 3006 to match HTTP packets with source addresses other than 10.2.1.1.

```
[Device] acl advanced 3006
[Device-acl-ipv4-adv-3006] rule 0 permit tcp destination-port eq www
[Device-acl-ipv4-adv-3006] quit
```

Configure Node 0 for policy **pbr1** to forward packets matching ACL 3005 to the next hop 10.5.1.2.

```
[Device] policy-based-route pbr1 permit node 0
[Device-pbr-pbr1-0] if-match acl 3005
[Device-pbr-pbr1-0] apply next-hop 10.5.1.2
[Device-pbr-pbr1-0] quit
```

Configure Node 1 for policy **pbr1** to forward packets matching ACL 3006 to the next hop 10.3.1.2.

```
[Device] policy-based-route pbr1 permit node 1
[Device-pbr-pbr1-1] if-match acl 3006
[Device-pbr-pbr1-1] apply next-hop 10.3.1.2
[Device-pbr-pbr1-1] quit
```

Apply policy **pbr1** to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip policy-based-route pbr1
[Device-Vlan-interface2] quit
```

Verifying the configuration

On Device, display PBR policy information.

```
[Device] display ip policy-based-route policy pbr1
Policy name: pbr1
  node 0 permit:
    if-match acl 3005
    apply next-hop 10.5.1.2
  node 1 permit:
    if-match acl 3006
    apply next-hop 10.3.1.2
```

The output shows that the PBR configurations are successful.

On Switch, display the path for forwarding non-HTTP packets with source address 10.1.1.1.

NOTE:

Before you use a **tracert** command, perform the following tasks:

- Enable sending of ICMP timeout packets on the intermediate devices.
- Enable sending of ICMP destination unreachable packets on the destination device.

```
<Switch> tracert -a 10.1.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.1.1.1, 30 hops at most, 52 bytes
 each packet, press CTRL+C to break
 1  10.1.2.1 (10.1.2.1)  2.178 ms  1.364 ms  1.058 ms
 2  10.4.1.2 (10.4.1.2)  1.548 ms  1.248 ms  1.112 ms
 3  192.168.1.1 (192.168.1.1)  1.594 ms  1.321 ms  1.093 ms
```

The output shows that non-HTTP packets with source address 10.1.1.1 are forwarded to the next hop 10.4.1.2.

On Switch, display the path for forwarding packets with source address 10.2.1.1.

```
<Switch> tracert -a 10.2.1.1 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1) from 10.2.1.1, 30 hops at most, 40 bytes
 each packet, press CTRL+C to break
 1  10.1.2.1 (10.1.2.1)  1.721 ms  1.226 ms  1.050 ms
 2  10.5.1.2 (10.5.1.2)  4.494 ms  1.385 ms  1.170 ms
 3  192.168.1.1 (192.168.1.1)  1.448 ms  1.304 ms  1.093 ms
```

The output shows that packets with source address 10.2.1.1 are forwarded to the next hop 10.5.1.2.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 1
#
vlan 2 to 5
#
```

```
policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 10.5.1.2
#
policy-based-route pbr1 permit node 1
 if-match acl 3006
 apply next-hop 10.3.1.2
#
interface Vlan-interface2
 ip address 10.1.2.1 255.255.255.0
 ip policy-based-route pbr1
#
interface Vlan-interface3
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface4
 ip address 10.4.1.1 255.255.255.0
#
interface Vlan-interface5
 ip address 10.5.1.1 255.255.255.0
#
ip route-static 192.168.1.0 24 10.3.1.2
 ip route-static 192.168.1.0 24 10.4.1.2 preference 40
 ip route-static 192.168.1.0 24 10.5.1.2
#
acl number 3005
 rule 0 permit ip source 10.2.1.1 0
#
acl number 3006
 rule 0 permit tcp destination-port eq www
#
```

Example: Configuring IPv6 PBR

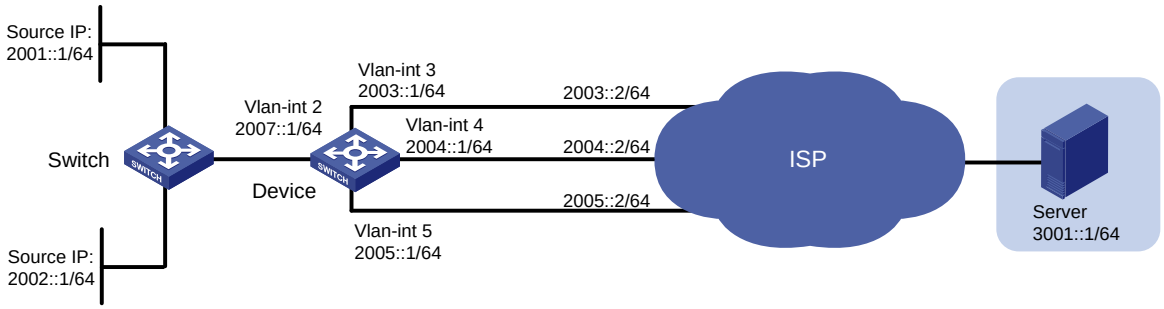
Network configuration

As shown in Figure 2, on Device, all packets destined for Server are forwarded to the next hop 2004::2 by default.

Configure IPv6 PBR to meet the following requirements:

- Packets with source IPv6 address 2002::1 received on VLAN-interface 2 are forwarded to the next hop 2005::2.
- HTTP packets with source IPv6 addresses other than 2002::1 received on VLAN-interface 2 are forwarded to the next hop 2003::2.

Figure 2 Network diagram



Analysis

To forward the two types of packets to different next hops, you must perform the following tasks:

- Configure two ACLs to classify the two types of packets.
- Configure two policy nodes to forward the packets to the specified next hops.

To ensure that packets with source address 2002::1 are forwarded to the next hop 2005::2, assign a node a smaller node ID to match the packets.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx

MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6658P01 and later

Procedures

Configure an IPv6 address for VLAN-interface 2.

```
<Device> system-view
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ipv6 address 2007::1 64
[Device-Vlan-interface2] quit
```

Configure IPv6 addresses for other interfaces in the same way VLAN-interface 2 is configured. (Details not shown.)

Configure three static routes and configure 2004::2/64 as the default next hop.

```
[Device] ipv6 route-static 3001::1 64 2003::2
[Device] ipv6 route-static 3001::1 64 2004::2 preference 40
[Device] ipv6 route-static 3001::1 64 2005::2
```

Create IPv6 ACL 3005 to match packets with source address 2002::1.

```
[Device] acl ipv6 advanced 3005
[Device-acl-ipv6-adv-3005] rule 0 permit ipv6 source 2002::1/128
[Device-acl-ipv6-adv-3005] quit
```

Create IPv6 ACL 3006 to match HTTP packets with source addresses other than 2002::1.

```
[Device] acl ipv6 advanced 3006
[Device-acl-ipv6-adv-3006] rule 0 permit tcp destination-port eq www
[Device-acl-ipv6-adv-3006] quit
```

Configure Node 0 for policy **pbr1** to forward packets matching IPv6 ACL 3005 to the next hop 2005::2.

```
[Device] ipv6 policy-based-route pbr1 permit node 0
[Device-pbr6-pbr1-0] if-match acl 3005
[Device-pbr6-pbr1-0] apply next-hop 2005::2
[Device-pbr6-pbr1-0] quit
```

Configure Node 1 for policy **pbr1** to forward packets matching IPv6 ACL 3006 to the next hop 2003::2.

```
[Device] ipv6 policy-based-route pbr1 permit node 1
[Device-pbr6-pbr1-1] if-match acl 3006
[Device-pbr6-pbr1-1] apply next-hop 2003::2
[Device-pbr6-pbr1-1] quit
```

Apply policy **pbr1** to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ipv6 policy-based-route pbr1
[Device-Vlan-interface2] quit
```

Verifying the configuration

On Device, display IPv6 PBR policy information.

```
[Device] display ipv6 policy-based-route policy pbr1
Policy name: pbr1
  node 0 permit:
    if-match acl 3005
    apply next-hop 2005::2
  node 1 permit:
    if-match acl 3006
    apply next-hop 2003::2
```

The output shows that the IPv6 PBR configurations are successful.

On Device, verify the forwarding of packets with source address 2002::1. (Details not shown.)

- If 2005::2 is reachable, packets are forwarded to the next hop 2005::2.
- If 2005::2 is not reachable, packets are forwarded to the next hop 2004::2.

On Device, verify the forwarding of HTTP packets. (Details not shown.)

- If 2003::2 is reachable, packets are forwarded to the next hop 2003::2.
- If 2003::2 is not reachable, packets are forwarded to the next hop 2004::2.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 1
#
vlan 2 to 5
#
ipv6 policy-based-route pbr1 permit node 0
 if-match acl 3005
 apply next-hop 2005::2
#
ipv6 policy-based-route pbr1 permit node 1
 if-match acl 3006
```

```
 apply next-hop 2003::2
#
interface Vlan-interface2
 ipv6 policy-based-route pbr1
 ipv6 address 2007::1/64
#
interface Vlan-interface3
 ipv6 address 2003::1 64
#
interface Vlan-interface4
 ipv6 address 2004::1 64
#
interface Vlan-interface5
 ipv6 address 2005::1 64
#
ipv6 route-static 3001:: 64 2003::2
 ipv6 route-static 3001:: 64 2004::2 preference 40
 ipv6 route-static 3001:: 64 2005::2
#
 acl ipv6 number 3005
 rule 0 permit ipv6 source 2002::1/128
#
 acl ipv6 number 3006
 rule 0 permit tcp destination-port eq www
#
```

Contents

Introduction

This document provides OSPFv3 route filtering configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of OSPFv3 route filtering.

Example: Configuring OSPFv3 route filtering

Network configuration

As shown in Figure 1, the devices of an enterprise reside in OSPFv3 and RIPng domains.

Configure route redistribution between OSPFv3 and RIPng to interconnect the devices.

Configure route filtering on Device E, Device C, and Device D to meet the following requirements:

- The route destined for R&D department 2 is not redistributed to OSPFv3.
- Marketing department 1 cannot reach R&D department 1.
- R&D department 1 and the After-sale service department cannot reach Marketing department 2.

Figure 1 Network diagram

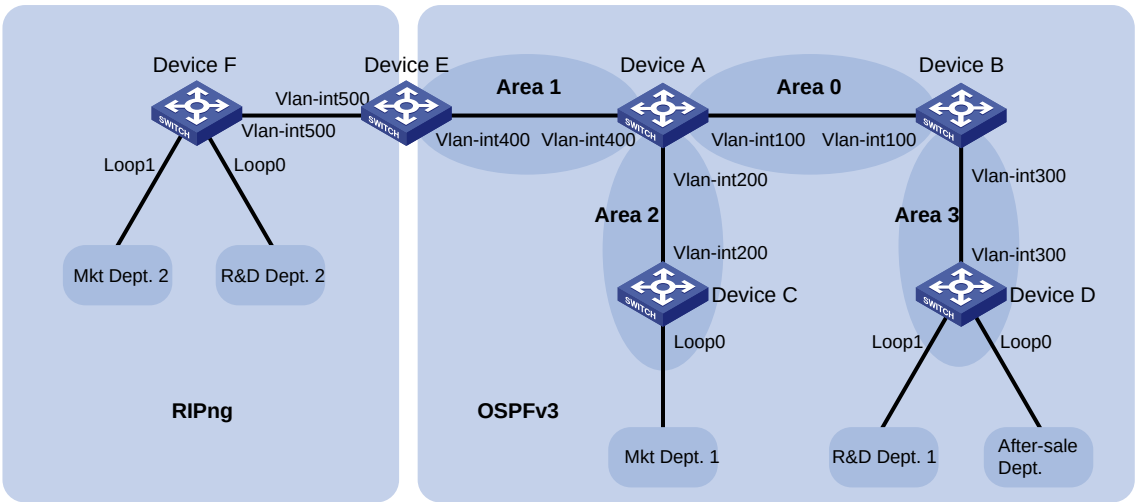


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int100	1::1/64	Device B	Vlan-int100	1::2/64
	Vlan-int200	2::1/64		Vlan-int300	3::1/64
	Vlan-int400	4::1/64			
Device C	Vlan-int200	2::2/64	Device D	Vlan-int300	3::2/64
	Loop0	13::1/64		Loop0	11::1/64
				Loop1	12::1/64
Device E	Vlan-int400	4::2/64	Device F	Vlan-int500	5::2/64
	Vlan-int500	5::1/64		Loop0	14::1/64
				Loop1	15::1/64

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series	Release 63xx

MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure OSPFv3 route filtering, follow these restrictions and guidelines:

- The **`filter-policy export`** command that filters redistributed routes takes effect only on an ASBR.
- OSPFv3 filters routes calculated using received LSAs. It does not filter LSAs.
- IP communication is bidirectional. If a router filters out a route destined for Network A, the subnets attached to the router cannot reach Network A, and Network A cannot reach the subnets.
- When you configure route filtering by referencing an ACL, configure the **`rule permit source any`** item following multiple **`rule deny source`** items to allow unmatched routes to pass.
- Specify a Router ID when you configure OSPFv3.

Procedures

Configuring IPv6 addresses

Configure an IPv6 address for VLAN-interface 100.

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ipv6 address 1::1 64
```

Configure IPv6 addresses for other interfaces in the same way VLAN-interface 100 is configured. (Details not shown.)

Configuring OSPFv3

Enable OSPFv3 on Device A.

```
<DeviceA> system-view
[DeviceA] ospfv3
[DeviceA-ospfv3-1] router-id 6.6.6.6
[DeviceA-ospfv3-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ospfv3 1 area 0
```

```
[DeviceA-Vlan-interface100] quit
[DeviceA] interface vlan-interface 200
[DeviceA-Vlan-interface200] ospfv3 1 area 2
[DeviceA-Vlan-interface200] quit
[DeviceA] interface vlan-interface 400
[DeviceA-Vlan-interface400] ospfv3 1 area 1
[DeviceA-Vlan-interface400] quit
# Enable OSPFv3 on Device B.
<DeviceB> system-view
[DeviceB] ospfv3
[DeviceB-ospfv3-1] router-id 5.5.5.5
[DeviceB-ospfv3-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ospfv3 1 area 0
[DeviceB-Vlan-interface100] quit
[DeviceB] interface vlan-interface 300
[DeviceB-Vlan-interface300] ospfv3 1 area 3
[DeviceB-Vlan-interface300] quit
```

Enable OSPFv3 on Device C.

```
<DeviceC> system-view
[DeviceC] ospfv3
[DeviceC-ospfv3-1] router-id 4.4.4.4
[DeviceC-ospfv3-1] quit
[DeviceC] interface vlan-interface 200
[DeviceC-Vlan-interface200] ospfv3 1 area 2
[DeviceC-Vlan-interface200] quit
[DeviceC] interface loopback 0
[DeviceC-LoopBack0] ospfv3 1 area 2
[DeviceC-LoopBack0] quit
```

Enable OSPFv3 on Device D.

```
<DeviceD> system-view
[DeviceD] ospfv3
[DeviceD-ospfv3-1] router-id 3.3.3.3
[DeviceD-ospfv3-1] quit
[DeviceD] interface vlan-interface 300
[DeviceD-Vlan-interface300] ospfv3 1 area 3
[DeviceD-Vlan-interface300] quit
[DeviceD] interface loopback 0
[DeviceD-LoopBack0] ospfv3 1 area 3
[DeviceD-LoopBack0] quit
[DeviceD] interface loopback 1
[DeviceD-LoopBack1] ospfv3 1 area 3
[DeviceD-LoopBack1] quit
```

Enable OSPFv3 on Device E.

```
<DeviceE> system-view
[DeviceE] ospfv3
[DeviceE-ospfv3-1] router-id 2.2.2.2
[DeviceE-ospfv3-1] quit
```

```
[DeviceE] interface vlan-interface 400
[DeviceE-Vlan-interface400] ospfv3 1 area 1
[DeviceE-Vlan-interface400] quit
```

Configure RIPng

Enable RIPng on Device E.

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] quit
[DeviceE] interface vlan-interface 500
[DeviceE-Vlan-interface500] ripng 1 enable
[DeviceE-Vlan-interface500] quit
```

Enable RIPng on Device F.

```
<DeviceF> system-view
[DeviceF] ripng
[DeviceF-ripng-1] quit
[DeviceF] interface vlan-interface 500
[DeviceF-Vlan-interface500] ripng 1 enable
[DeviceF-Vlan-interface500] quit
[DeviceF] interface loopback 0
[DeviceF-LoopBack0] ripng 1 enable
[DeviceF-LoopBack0] quit
[DeviceF] interface loopback 1
[DeviceF-LoopBack0] ripng 1 enable
[DeviceF-LoopBack0] quit
```

Configuring route redistribution

Configure Device E to redistribute OSPFv3 and direct routes to RIPng.

```
<DeviceE> system-view
[DeviceE] ripng
[DeviceE-ripng-1] import-route direct
[DeviceE-ripng-1] import-route ospfv3
[DeviceE-ripng-1] quit
```

Configure Device E to redistribute RIPng and direct routes to OSPFv3.

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] import-route direct
[DeviceE-ospfv3-1] import-route ripng
[DeviceE-ospfv3-1] quit
```

Verify that Device E has routes to all networks.

```
[DeviceE] display ipv6 routing-table

Destinations : 15        Routes : 15

Destination: ::1/128                                Protocol  : Direct
NextHop    : ::1                                    Preference: 0
Interface  : InLoop0                                Cost      : 0
```

```
Destination: 1::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 2

Destination: 2::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 2

Destination: 3::/64                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 3

Destination: 4::/64                                  Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : Vlan400                                 Cost      : 0

Destination: 4::2/128                                Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 5::/64                                  Protocol  : Direct
NextHop    : ::                                      Preference: 0
Interface  : Vlan500                                 Cost      : 0

Destination: 5::1/128                                Protocol  : Direct
NextHop    : ::1                                     Preference: 0
Interface  : InLoop0                                 Cost      : 0

Destination: 11::1/128                               Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 3

Destination: 12::1/128                               Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 3

Destination: 13::1/128                               Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:124D                Preference: 10
Interface  : Vlan400                                 Cost      : 2

Destination: 14::/64                                 Protocol  : RIPng
NextHop    : FE80::2E0:FCFF:FE11:19B5                Preference: 100
Interface  : Vlan500                                 Cost      : 1

Destination: 15::/64                                 Protocol  : RIPng
NextHop    : FE80::2E0:FCFF:FE11:19B5                Preference: 100
Interface  : Vlan500                                 Cost      : 1
```

```
Destination: FE80::/10                                  Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: FF00::/8                                   Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : NULL0                                      Cost      : 0
```

Verify that other devices have routes to all networks. (Details not shown.)

Configuring OSPFv3 route filtering

On Device C, configure IPv6 basic ACL 2000 to permit any subnet except 12::1/64.

```
<DeviceC> system-view
[DeviceC] acl ipv6 basic 2000
[DeviceC-acl-ipv6-basic-2000] rule 0 deny source 12::1 64
[DeviceC-acl-ipv6-basic-2000] rule permit source any
[DeviceC-acl-ipv6-basic-2000] quit
```

On Device C, use ACL 2000 to filter received routes.

```
[DeviceC] ospfv3
[DeviceC-ospfv3-1] filter-policy 2000 import
[DeviceC-ospfv3-1] quit
```

On Device D, configure IPv6 basic ACL 2000 to permit any subnet except 15::1/64.

```
<DeviceD> system-view
[DeviceD] acl ipv6 basic 2000
[DeviceD-acl-ipv6-basic-2000] rule 0 deny source 15::1 64
[DeviceD-acl-ipv6-basic-2000] rule permit source any
[DeviceD-acl-ipv6-basic-2000] quit
```

On Device D, use ACL 2000 to filter received routes.

```
[DeviceD] ospfv3
[DeviceD-ospfv3-1] filter-policy 2000 import
[DeviceD-ospfv3-1] quit
```

On Device E, configure IPv6 basic ACL 2000 to permit any subnet except 14::1/64.

```
<DeviceE> system-view
[DeviceE] acl ipv6 basic 2000
[DeviceE-acl-ipv6-basic-2000] rule 0 deny source 14::1 64
[DeviceE-acl-ipv6-basic-2000] rule permit source any
[DeviceE-acl-ipv6-basic-2000] quit
```

On Device E, use ACL 2000 to filter routes redistributed from RIPng.

```
[DeviceE] ospfv3
[DeviceE-ospfv3-1] filter-policy 2000 export ripng 1
[DeviceE-ospfv3-1] quit
```

Verifying the configuration

Verify that Device C does not have a route to 12::/64.

```
[DeviceC] display ipv6 routing-table
```

```
Destinations : 13        Routes : 13

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 1::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 10
Interface  : Vlan200                                    Cost      : 2

Destination: 2::/64                                     Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Vlan200                                    Cost      : 0

Destination: 2::2/128                                   Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 3::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 10
Interface  : Vlan200                                    Cost      : 3

Destination: 4::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 10
Interface  : Vlan200                                    Cost      : 2

Destination: 5::/64                                     Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 150
Interface  : Vlan200                                    Cost      : 1

Destination: 11::1/128                                  Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 10
Interface  : Vlan200                                    Cost      : 3

Destination: 13::/64                                    Protocol  : Direct
NextHop    : ::                                         Preference: 0
Interface  : Loop0                                      Cost      : 0

Destination: 13::1/128                                  Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Destination: 15::/64                                    Protocol  : OSPFv3
NextHop    : FE80::2E0:FCFF:FE58:1245                   Preference: 150
Interface  : Vlan200                                    Cost      : 1

Destination: FE80::/10                                  Protocol  : Direct
```

```
NextHop    : ::                                    Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: FF00::/8                              Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : NULL0                                 Cost      : 0
```

Verify that Marketing department 1 cannot reach R&D department 1.

```
[DeviceC] ping ipv6 -a 13::1 12::1
Ping6(56 data bytes) 13::1 --> 12::1, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 12::1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Verify that Device D does not have a route to 15::/64.

```
[DeviceD] display ipv6 routing-table

Destinations : 14        Routes : 14

Destination: ::1/128                               Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 1::/64                                Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815              Preference: 10
Interface  : Vlan300                               Cost      : 2

Destination: 2::/64                                Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815              Preference: 10
Interface  : Vlan300                               Cost      : 3

Destination: 3::/64                                Protocol  : Direct
NextHop    : ::                                    Preference: 0
Interface  : Vlan300                               Cost      : 0

Destination: 3::2/128                              Protocol  : Direct
NextHop    : ::1                                   Preference: 0
Interface  : InLoop0                               Cost      : 0

Destination: 4::/64                                Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815              Preference: 10
Interface  : Vlan300                               Cost      : 3

Destination: 5::/64                                Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815              Preference: 150
```

```
Interface  : Vlan300                                  Cost      : 1

Destination: 11::/64                                  Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Loop0                                    Cost      : 0

Destination: 11::1/128                                Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 12::/64                                  Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : Loop1                                    Cost      : 0

Destination: 12::1/128                                Protocol  : Direct
NextHop    : ::1                                      Preference: 0
Interface  : InLoop0                                  Cost      : 0

Destination: 13::1/128                                Protocol  : OSPFv3
NextHop    : FE80::2A0:FCFF:FE00:5815                 Preference: 10
Interface  : Vlan300                                  Cost      : 3

Destination: FE80::/10                                Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0                                    Cost      : 0

Destination: FF00::/8                                 Protocol  : Direct
NextHop    : ::                                       Preference: 0
Interface  : NULL0                                    Cost      : 0
```

Verify that the After-sale service department cannot reach Marketing department 2.

```
[DeviceD] ping ipv6 -a 11::1 15::1
Ping6(56 data bytes) 11::1 --> 15::1, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping6 statistics for 15::1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

Verify that R&D department 1 cannot reach Marketing department 2.

```
[DeviceD] ping ipv6 -a 12::1 15::1
Ping6(56 data bytes) 12::1 --> 15::1, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
```

```
--- Ping6 statistics for 15::1 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

The output on Device C and Device D shows that Device E has filtered out the route destined for R&D development 2.

Configuration files

- Device A:

```
#
ospfv3 1
 router-id 6.6.6.6
 area 0.0.0.0
 area 0.0.0.1
 area 0.0.0.2
#
vlan 100
#
vlan 200
#
vlan 400
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 address 1::1/64
#
interface Vlan-interface200
 ospfv3 1 area 0.0.0.2
 ipv6 address 2::1/64
#
interface Vlan-interface400
 ospfv3 1 area 0.0.0.1
 ipv6 address 4::1/64
#
```

- Device B:

```
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
 area 0.0.0.3
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
 ipv6 address 1::2/64
```

```
#
interface Vlan-interface300
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::1/64
#
```

- Device C:

```
#
ospfv3 1
 router-id 4.4.4.4
 filter-policy 2000 import
 area 0.0.0.2
#
vlan 200
#
interface LoopBack0
 ospfv3 1 area 0.0.0.2
 ipv6 address 13::1/64
#
interface Vlan-interface200
 ospfv3 1 area 0.0.0.2
 ipv6 address 2::2/64
#
acl ipv6 basic 2000
 rule 0 deny source 12::/64
 rule 5 permit
#
```

- Device D:

```
#
ospfv3 1
 router-id 3.3.3.3
 filter-policy 2000 import
 area 0.0.0.3
#
vlan 300
#
interface LoopBack0
 ospfv3 1 area 0.0.0.3
 ipv6 address 11::1/64
#
interface LoopBack1
 ospfv3 1 area 0.0.0.3
 ipv6 address 12::1/64
#
interface Vlan-interface300
 ospfv3 1 area 0.0.0.3
 ipv6 address 3::2/64
#
acl ipv6 basic 2000
```

```
 rule 0 deny source 15::/64
 rule 5 permit
#
```

- Device E:

```
#
ospfv3 1
 router-id 2.2.2.2
 import-route direct
import-route ripng 1
 filter-policy 2000 export ripng 1
 area 0.0.0.1
#
ripng 1
 import-route direct
 import-route ospfv3 1
#
vlan 400
#
vlan 500
#
interface Vlan-interface400
 ospfv3 1 area 0.0.0.1
 ipv6 address 4::2/64
#
interface Vlan-interface500
 ipv6 address 5::1/64
 ripng 1 enable
#
acl ipv6 basic 2000
 rule 0 deny source 14::/64
 rule 5 permit
#
```

- Device F:

```
#
ripng 1
#
vlan 500
#
interface LoopBack0
 ipv6 address 14::1/64
 ripng 1 enable
#
interface LoopBack1
 ipv6 address 15::1/64
 ripng 1 enable
#
interface Vlan-interface500
 ipv6 address 5::2/64
```

```
 ripng 1 enable
#
```

Contents

Introduction

This document provides IPv6 IS-IS configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IPv6 IS-IS.

Example: Configuring IPv6 IS-IS

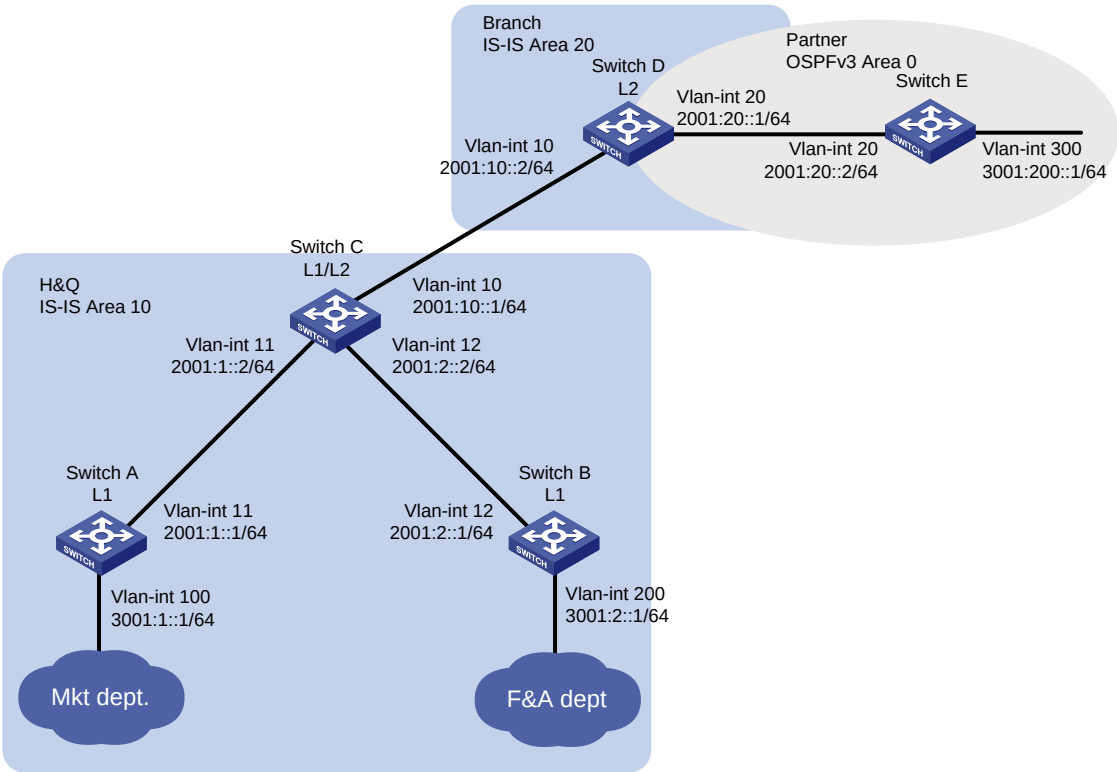
Network configuration

As shown in Figure 1, the company's headquarters and the branch run IPv6 IS-IS. The partner runs OSPFv3.

Configure the switches to meet the following requirements:

- The Marketing department can reach the Finance department, the branch, and the partner.
- The Finance department and the branch cannot reach each other, and the branch does not have a route to the Finance department.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure Switch A and Switch B in Area 10 as Level-1 routers to allow communication between the Marketing department and the Finance department.
- Configure route redistribution between IPv6 IS-IS and OSPFv3 on Switch D to allow communication between the Marketing department and the partner.
- Configure Switch C to use a prefix list to advertise only network 3001:1::/64 to Level-2. So that the branch does not have a route to the Finance department.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series	Release 63xx

S5560S-SI switch series	
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported

IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Configuring Switch A

Configure an IPv6 address for VLAN-interface 11.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ipv6 address 2001:1::1 64
[SwitchA-Vlan-interface11] quit
```

Configure IPv6 addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IPv6 IS-IS.

```
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.3001.0001.0001.00
[SwitchA-isis-1] address-family ipv6
[SwitchA-isis-1-ipv6] quit
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 11
[SwitchA–vlan-interface 11] isis ipv6 enable 1
[SwitchA–vlan-interface 11] quit
[SwitchA] interface vlan-interface 100
[SwitchA–Vlan-interface100] isis ipv6 enable 1
[SwitchA–Vlan-interface100] quit
```

Configuring Switch B

Configure an IPv6 address for VLAN-interface 12.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 12
[SwitchB-Vlan-interface12] ipv6 address 2001:2::1 64
[SwitchB-Vlan-interface12] quit
```

Configure IPv6 addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IPv6 IS-IS.

```
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.3001.0002.0001.00
[SwitchB-isis-1] address-family ipv6
[SwitchB-isis-1-ipv6] quit
```

```
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 12
[SwitchB–Vlan-interface12] isis ipv6 enable 1
[SwitchB–Vlan-interface12] quit
[SwitchB] interface vlan-interface 200
[SwitchB–Vlan-interface 200] isis ipv6 enable 1
[SwitchB–Vlan-interface 200] quit
```

Configuring Switch C

Configure an IPv6 address for VLAN-interface 11.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 11
[SwitchC-Vlan-interface11] ipv6 address 2001:1::2 64
[SwitchC-Vlan-interface11] quit
```

Configure IPv6 addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IPv6 IS-IS.

```
[SwitchC] isis 1
[SwitchC-isis-1] is-level level-1
[SwitchC-isis-1] network-entity 10.2001.0010.0001.00
[SwitchC-isis-1] address-family ipv6
[SwitchC-isis-1-ipv6] quit
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 10
[SwitchC–Vlan-interface10] isis ipv6 enable 1
[SwitchC–Vlan-interface10] quit
[SwitchC] interface vlan-interface 11
[SwitchC–Vlan-interface11] isis ipv6 enable 1
[SwitchC–Vlan-interface11] quit
[SwitchC] interface vlan-interface 12
[SwitchC–Vlan-interface12] isis ipv6 enable 1
[SwitchC–Vlan-interface12] quit
```

Configure route leaking from Level-1 to Level-2, and use prefix list 1 to advertise only network 3001:1::/64 to Level-2.

```
[SwitchC] ipv6 prefix-list 1 permit 3001:1:: 64
[SwitchC] isis 1
[SwitchC-isis-1] address-family ipv6
[SwitchC-isis-1-ipv6] import-route isisv6 level-1 into level-2 filter-policy prefix-list
1
[SwitchC-isis-1-ipv6] quit
[SwitchC-isis-1] quit
```

Configuring Switch D

Configure an IPv6 address for VLAN-interface 10.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 10
[SwitchD-Vlan-interface10] ipv6 address 2001:10::2 64
```

```
[SwitchD-Vlan-interface10] quit
```

Configure IPv6 addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure IPv6 IS-IS.

```
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.2001.0020.0001.00
[SwitchD-isis-1] address-family ipv6
[SwitchD-isis-1-ipv6] quit
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 10
[SwitchD–Vlan-interface10] isis ipv6 enable 1
[SwitchD–Vlan-interface10] quit
[SwitchD] interface vlan-interface 20
[SwitchD–Vlan-interface20] isis ipv6 enable 1
[SwitchD–Vlan-interface20] quit
```

Configure OSPFv3.

```
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 20
[SwitchD–Vlan-interface20] ospfv3 1 area 0
[SwitchD–Vlan-interface20] quit
```

Redistribute OSPFv3 and direct routes into IPv6 IS-IS.

```
[SwitchD] isis 1
[SwitchD-isis-1] address-family ipv6
[SwitchD-isis-1-ipv6] import-route ospfv3
[SwitchD-isis-1-ipv6] import-route direct
[SwitchD-isis-1-ipv6] quit
[SwitchD-isis-1] quit
```

Redistribute IPv6 IS-IS and direct routes into OSPFv3.

```
[SwitchD] ospfv3 1
[SwitchD-ospfv3-1] import-route isisv6 1
[SwitchD-ospfv3-1] import-route direct
```

Configuring Switch E

Configure an IPv6 address for VLAN-interface 20.

```
<SwitchE> system-view
[SwitchE] interface vlan-interface20
[SwitchE-Vlan-interface12] ipv6 address 2001:20::2 64
[SwitchE-Vlan-interface12] quit
```

Configure IPv6 addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configure OSPFv3.

```
[SwitchE] ospfv3
[SwitchE-ospfv3-1] router-id 5.5.5.5
[SwitchE-ospfv3-1] quit
[SwitchE] interface vlan-interface 20
```

```
[SwitchE–Vlan-interface 20] ospfv3 1 area 0
[SwitchE–Vlan-interface 20] quit
[SwitchE] interface vlan-interface 300
[SwitchE–Vlan-interface 300] ospfv3 1 area 0
[SwitchE–Vlan-interface 300] quit
```

Verifying the configuration

Verify that the branch can reach the Marketing department, but cannot reach the Finance department.

```
[SwitchD] display isis route ipv6
                        Route information for IS-IS(1)
                        ------------------------------
                        Level-2 IPv6 Forwarding Table
                        ------------------------------

 Destination : 2001:10::                              PrefixLen: 64
 Flag        : D/L/-                                  Cost     : 10
 Next Hop    : Direct                                 Interface: Vlan10
 Destination : 2001:1::                               PrefixLen: 64
 Flag        : R/-/-                                  Cost     : 20
 Next Hop    : FE80::7625:8AFF:FE02:4D13              Interface: Vlan10
 Destination : 2001:2::                               PrefixLen: 64
 Flag        : R/-/-                                  Cost     : 20
 Next Hop    : FE80::7625:8AFF:FE02:4D13              Interface: Vlan10
 Destination : 3001:1::                               PrefixLen: 64
 Flag        : R/-/-                                  Cost     : 30
 Next Hop    : FE80::7625:8AFF:FE02:4D13              Interface: Vlan10
      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Verify that the company can communicate with the partner.

- Display the IPv6 IS-IS routing table on Switch C.

```
[SwitchC] display isis route ipv6 level-2
                        Route information for IS-IS(1)
                        ------------------------------
                        Level-2 IPv6 Forwarding Table
                        ------------------------------

 Destination : 2001:10::                              PrefixLen: 64
 Flag        : D/L/-                                  Cost     : 10
 Next Hop    : Direct                                 Interface: Vlan10
 Destination : 2001:1::                               PrefixLen: 64
 Flag        : D/L/-                                  Cost     : 10
 Next Hop    : Direct                                 Interface: Vlan11
 Destination : 2001:2::                               PrefixLen: 64
 Flag        : D/L/-                                  Cost     : 10
 Next Hop    : Direct                                 Interface: Vlan12
 Destination : 2001:20::                              PrefixLen: 64
 Flag        : R/L/-                                  Cost     : 20
 Next Hop    : FE80::BAAF:67FF:FE30:3304              Interface: Vlan10
 Destination : 3001:200::                             PrefixLen: 64
```

```
 Flag        : R/-/-                                  Cost     : 20
 Next Hop    : FE80::BAAF:67FF:FE30:3304              Interface: Vlan10
      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

- Ping 3001:200::1 from Switch A.

```
[SwitchA] ping ipv6 –a 3001:1::1 3001:200::1
Ping6(56 data bytes) 3001:1::1 --> 3001:200::1, press CTRL+C to break
56 bytes from 3001:200::1, icmp_seq=0 hlim=63 time=7.230 ms
56 bytes from 3001:200::1, icmp_seq=1 hlim=63 time=3.449 ms
56 bytes from 3001:200::1, icmp_seq=2 hlim=63 time=2.779 ms
56 bytes from 3001:200::1, icmp_seq=3 hlim=63 time=2.652 ms
56 bytes from 3001:200::1, icmp_seq=4 hlim=63 time=2.558 ms
--- Ping6 statistics for 3001:200::1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.558/3.734/7.230/1.776 ms
```

Configuration files

- Switch A:

```
#
isis 1
 is-level level-1
 network-entity 10.3001.0001.0001.00
 #
 address-family ipv6 unicast
#
vlan 11
#
vlan 100
#
interface Vlan-interface11
 isis ipv6 enable 1
 ipv6 address 2001:1::1/64
#
interface Vlan-interface100
 isis ipv6 enable 1
 ipv6 address 3001:1::1/64
#
```

- Switch B:

```
#
isis 1
 is-level level-1
 network-entity 10.3001.0002.0001.00
 #
 address-family ipv6 unicast
#
vlan 12
#
vlan 200
```

```
#
interface Vlan-interface12
 isis ipv6 enable 1
 ipv6 address 2001:2::1/64
#
interface Vlan-interface200
 isis ipv6 enable 1
 ipv6 address 3001:2::1/64
#
```

- Switch C:

```
#
isis 1
 network-entity 10.2001.0010.0001.00
 #
 address-family ipv6 unicast
  import-route isisv6 level-1 into level-2 filter-policy prefix-list 1
#
vlan 10 to 12
#
interface Vlan-interface10
 isis ipv6 enable 1
 ipv6 address 2001:10::1/64
#
interface Vlan-interface11
 isis ipv6 enable 1
 ipv6 address 2001:1::2/64
#
interface Vlan-interface12
 isis ipv6 enable 1
 ipv6 address 2001:2::2/64
#
 ipv6 prefix-list 1 index 10 permit 3001:1:: 64
#
```

- Switch D:

```
#
isis 1
 is-level level-2
 network-entity 20.2001.0020.0001.00
#
 address-family ipv6 unicast
 import-route direct
 import-route ospfv3 1
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
 import-route direct
 import-route isisv6 1
```

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 isis ipv6 enable 1
 ipv6 address 2001:10::2/64
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 address 2001:20::1/64
#
```

- Switch E:

```
#
ospfv3 1
 router-id 5.5.5.5
 area 0.0.0.0
#
vlan 20
#
vlan 300
#
interface Vlan-interface20
 ospfv3 1 area 0
 ipv6 address 2001:20::2/64
#
interface Vlan-interface300
 ospfv3 1 area 0
 ipv6 address 3001:200::1/64
#
```

Contents

Introduction

This document provides routing policy configuration examples.

Routing policies control routing paths by filtering and modifying routing information. Routing policies can filter advertised, received, and redistributed routes, and modify attributes for specific routes.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of routing polices.

Example: Configuring routing polices

Network configuration

As shown in Figure 1, a company's two departments reside in different ASs. Device A and Device F are the egress devices of the two departments. OSPF is the IGP protocol in AS 100.

- Configure BGP to make the two departments reachable to each other.
- Configure routing polices to specify the link Device B<—>Device C<—>Device D as the primary link to forward traffic between Device A and Device F. When the primary link fails, the link Device B<—>Device E<—>Device D forwards the traffic.

Figure 1 Network diagram

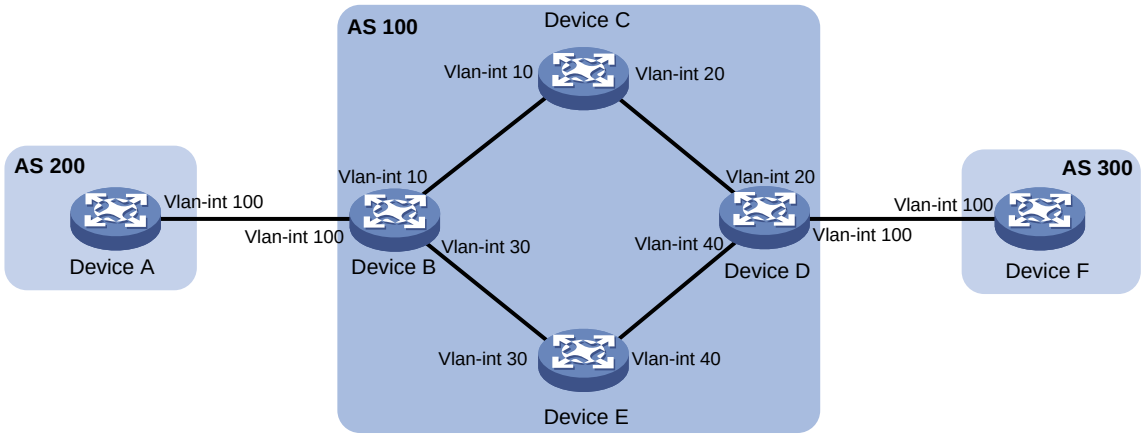


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int100	120.1.0.1/24	Device D	Vlan-int20	10.2.0.101/24
Device B	Vlan-int10	10.1.0.101/24		Vlan-int40	13.1.1.101/24
	Vlan-int30	192.168.0.101/24		Vlan-int100	120.2.0.2/24

Device	Interface	IP address	Device	Interface	IP address
	Vlan-int100	120.1.0.2/24	Device E	Vlan-int30	192.168.0.102/24
Device C	Vlan-int10	10.1.0.102/24		Vlan-int40	13.1.1.102/24
	Vlan-int20	10.2.0.102/24	Device F	Vlan-int100	120.2.0.1/24

Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the link Device B<—>Device C<—>Device D as the primary link:
  - On Device B, set the local preference to 200 for the path Device D—>Device C—>Device B. The path Device D—>Device E—>Device B uses the default local preference 100.
  - On Device D, set the local preference to 200 for the path Device B—>Device C—>Device D. The path Device B—>Device E—>Device D uses the default local preference 100.
- Set a higher preference for IBGP routes to ensure that IBGP routes rather than OSPF external routes are used in AS 100.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S6520-SI switch series	
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series	Not supported

MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Configuring IP addresses

Configure an IP address for VLAN-interface 100.

```
<DeviceA> system-view
[DeviceA] interface vlan-interface100
[DeviceA-Vlan-interface100] ip address 120.1.0.1 24
[DeviceA-Vlan-interface100] quit
```

Configure IP addresses for other interfaces, as shown in Figure 1. (Details not shown.)

Configuring OSPF

Configuring Device B

```
<DeviceB> system-view
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Configuring Device C

```
<DeviceC> system-view
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
```

```
[DeviceC-ospf-1] quit
```

Configuring Device D

```
<DeviceD> system-view
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Configuring Device E

```
<DeviceE> system-view
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

Configuring BGP

Configuring Device A

Enable BGP, set the local AS number to 200, and configure the router ID for BGP as 1.1.1.1.

```
<DeviceA> system-view
[DeviceA] bgp 200
[DeviceA-bgp-default] router-id 1.1.1.1
```

Establish an EBGP connection with Device B.

```
[DeviceA-bgp-default] peer 120.1.0.2 as-number 100
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceA-bgp-default] address-family ipv4 unicast
```

Enable Device A to exchange IPv4 unicast routing information with peer 120.1.0.2.

```
[DeviceA-bgp-default-ipv4] peer 120.1.0.2 enable
```

Inject network 120.1.0.0/24 to the BGP routing table.

```
[DeviceA-bgp-default-ipv4] network 120.1.0.0 255.255.255.0
[DeviceA-bgp-default-ipv4] quit
```

Configuring Device B

Enable BGP, set the local AS number to 100, and configure the router ID for BGP as 2.2.2.2.

```
<DeviceB> system-view
[DeviceB] bgp 100
[DeviceB-bgp-default] router-id 2.2.2.2
```

Establish an EBGP connection with Device A.

```
[DeviceB-bgp-default] peer 120.1.0.1 as-number 200
```

Establish IBGP connections with Device D.

```
[DeviceB-bgp-default] peer 10.2.0.101 as-number 100
[DeviceB-bgp-default] peer 13.1.1.101 as-number 100
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceB-bgp-default] address-family ipv4 unicast
```

Enable Device B to exchange IPv4 unicast routing information with peer 10.2.0.101.

```
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 enable
```

Specify Device B as the next hop for routes sent to peer 10.2.0.101.

```
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 next-hop-local
```

Enable Device B to exchange IPv4 unicast routing information with peer 13.1.1.101.

```
[DeviceB-bgp-default-ipv4] peer 13.1.1.101 enable
```

Specify Device B as the next hop for routes sent to peer 13.1.1.101.

```
[DeviceB-bgp-default-ipv4] peer 13.1.1.101 next-hop-local
```

Enable Device B to exchange IPv4 unicast routing information with peer 120.1.0.1.

```
[DeviceB-bgp-default-ipv4] peer 120.1.0.1 enable
[DeviceB-bgp-default-ipv4] quit
```

Configuring Device D

Enable BGP, set the local AS number to 100, and configure the router ID for BGP as 4.4.4.4.

```
<DeviceD> system-view
[DeviceD] bgp 100
[DeviceD-bgp-default] router-id 4.4.4.4
```

Establish IBGP connections with Device B.

```
[DeviceD-bgp-default] peer 10.1.0.101 as-number 100
[DeviceD-bgp-default] peer 192.168.0.101 as-number 100
```

Establish an EBGP connection with Device F.

```
[DeviceD-bgp-default] peer 120.2.0.1 as-number 300
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceD-bgp-default] address-family ipv4 unicast
```

Enable Device D to exchange IPv4 unicast routing information with peer 10.1.0.101.

```
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 enable
```

Specify Device D as the next hop for routes sent to peer 10.1.0.101.

```
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 next-hop-local
```

Enable Device D to exchange IPv4 unicast routing information with peer 192.168.0.101.

```
[DeviceD-bgp-default-ipv4] peer 192.168.0.101 enable
```

Specify Device D as the next hop for routes sent to peer 192.168.0.101.

```
[DeviceD-bgp-default-ipv4] peer 192.168.0.101 next-hop-local
```

Enable Device D to exchange IPv4 unicast routing information with peer 120.2.0.1.

```
[DeviceD-bgp-default-ipv4] peer 120.2.0.1 enable
[DeviceD-bgp-default-ipv4] quit
```

Configuring Device F

Enable BGP, set the local AS number to 300, and configure the router ID for BGP as 6.6.6.6.

```
<DeviceF> system-view
[DeviceF] bgp 300
[DeviceF-bgp-default] router-id 6.6.6.6
```

Establish an EBGP connection with Device D.

```
[DeviceF-bgp-default] peer 120.2.0.2 as-number 100
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceF-bgp-default] address-family ipv4 unicast
```

Inject network 120.2.0.0/24 to the BGP routing table.

```
[DeviceF-bgp-default-ipv4] network 120.2.0.0 255.255.255.0
```

Enable Device F to exchange IPv4 unicast routing information with peer 120.2.0.2.

```
[DeviceF-bgp-default-ipv4] peer 120.2.0.2 enable
[DeviceF-bgp-default-ipv4] quit
```

Verify BGP peer information on Device B.

```
[DeviceB] display bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 100
 Total number of peers: 3                 Peers in established state: 3

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.0.101             100        6        4    0       1 00:00:56 Established
  13.1.1.101             100        6        5    0       1 00:00:56 Established
  120.1.0.1              200        6        5    0       1 00:00:56 Established
```

The output shows that Device B has established two IBGP connections with Device D, and an EBGP connection with Device A. The connections are all in Established state.

Test the network connectivity between Device A and Device F.

```
[DeviceA] ping 120.2.0.1
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL+C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms

--- Ping statistics for 120.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

The output shows that Device A and Device F can reach each other.

Configuring routing polices

Configuring Device B

Configure ACL 2000 to permit route 120.1.0.0/24.

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-ipv4-basic-2000] quit
```

Configure routing policy **local-pre** to set the local preference to 200 for route 120.1.0.0/24.

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceB-route-policy-local-pre-10] apply local-preference 200
```

```
[DeviceB-route-policy-local-pre-10] quit
```

Apply routing policy **local-pre** to routes outgoing to peer 10.2.0.101.

```
[DeviceB] bgp 100
[DeviceB-bgp-default] address-family ipv4 unicast
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 route-policy local-pre export
```

Set the preference for IBGP routes to 100 (higher than the default preference of OSPF external routes 150).

```
[DeviceB-bgp-default-ipv4] preference 255 100 130
[DeviceB-bgp-default-ipv4] quit
```

Configuring Device D

Configure ACL 2000 to permit route 120.2.0.0/24.

```
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule permit source 120.2.0.0 0.0.0.255
[DeviceD-acl-ipv4-basic-2000] quit
```

Configure routing policy **local-pre** to set the local preference to 200 for route 120.2.0.0/24.

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre-10] if-match ip address acl 2000
[DeviceD-route-policy-local-pre-10] apply local-preference 200
[DeviceD-route-policy-local-pre-10] quit
```

Apply routing policy **local-pre** to routes outgoing to peer 10.1.0.101.

```
[DeviceD] bgp 100
[DeviceD-bgp-default] address-family ipv4 unicast
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 route-policy local-pre export
```

Set the preference for IBGP routes to 100 (higher than the default preference of OSPF external routes 150).

```
[DeviceD-bgp-default-ipv4] preference 255 100 130
[DeviceD-bgp-default-ipv4] quit
```

Verifying the configuration

On Device B, display the BGP routing table.

```
[DeviceB] display bgp routing-table ipv4

 Total number of routes: 3

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 120.1.0.0/24       120.1.0.1       0                     0       200i
* >i 120.2.0.0/24       10.2.0.101      0          200        0       300i
*  i                    13.1.1.101      0          100        0       300i
```

The output shows that Device B has two routes to 120.2.0.0/24 with local preferences 100 and 200.

Trace the path that traffic traverses from Device A to Device F.

```
[DeviceA] tracert 120.2.0.1
traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, press CTRL+C
to break
 1  120.1.0.2 (120.1.0.2)  2.208 ms  1.119 ms  1.085 ms
 2  10.1.0.102 (10.1.0.102)  1.083 ms  1.100 ms  1.085 ms
 3  10.2.0.101 (10.2.0.101)  2.364 ms  1.099 ms  1.086 ms
 4  120.2.0.1 (120.2.0.1)  3.825 ms  3.693 ms  4.008 ms
```

The output shows that traffic is forwarded along the path Device A—>Device B—>Device C—>Device D—>Device F.

When the primary link fails, display the BGP routing table on Device B.

```
[DeviceB] display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 120.1.0.0/24       120.1.0.1       0                     0       200i
* >i 120.2.0.0/24       13.1.1.101      0          100        0       300i
```

The output shows that Device B has one route to 120.2.0.0/24.

Trace the path that traffic traverses from Device A to Device F.

```
[DeviceA] tracert 120.2.0.1
traceroute to 120.2.0.1 (120.2.0.1), 30 hops at most, 52 bytes each packet, press CTRL+C
to break
 1  120.1.0.2 (120.1.0.2)  2.308 ms  1.127 ms  1.091 ms
 2  192.168.0.102 (192.168.0.102)  1.086 ms  1.102 ms  1.096 ms
 3  13.1.1.101 (13.1.1.101)  2.451 ms  2.087 ms  1.092 ms
 4  120.2.0.1 (120.2.0.1)  3.533 ms  3.818 ms  4.002 ms
```

The output shows that traffic is forwarded along the path Device A—>Device B—>Device E—>Device D—>Device F.

Configuration files

- Device A:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 120.1.0.1 255.255.255.0
#
```

```
bgp 200
 router-id 1.1.1.1
 peer 120.1.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.1.0.0 255.255.255.0
  peer 120.1.0.2 enable
#
```

- Device B:

```
#
ospf 1
import-route direct
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
vlan 10
#
vlan 30
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.101 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.0.101 255.255.255.0
#
interface Vlan-interface100
 ip address 120.1.0.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 13.1.1.101 as-number 100
 peer 120.1.0.1 as-number 200
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.2.0.101 enable
  peer 10.2.0.101 next-hop-local
  peer 10.2.0.101 route-policy local-pre export
  peer 13.1.1.101 enable
  peer 13.1.1.101 next-hop-local
  peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
```

```
 apply local-preference 200
#
acl number 2000
 rule 0 permit source 120.1.0.0 0.0.0.255
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
#
interface Vlan-interface20
 ip address 10.2.0.102 255.255.255.0
#
```

- Device D:

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 20
#
vlan 40
#
vlan 100
#
interface Vlan-interface20
ip address 10.2.0.101 255.255.255.0
#
interface Vlan-interface40
 ip address 13.1.1.101 255.255.255.0
#
interface Vlan-interface100
 ip address 120.2.0.2 255.255.255.0
#
bgp 100
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100
```

```
 peer 120.2.0.1 as-number 300
 peer 192.168.0.101 as-number 100
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local
  peer 10.1.0.101 route-policy local-pre export
  peer 192.168.0.101 enable
  peer 192.168.0.101 next-hop-local
  peer 120.2.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
acl number 2000
 rule 0 permit source 120.2.0.0 0.0.0.255
#
```

- Device E:

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
vlan 30
#
vlan 40
#
interface Vlan-interface30
 ip address 192.168.0.102 255.255.255.0
#
interface Vlan-interface40
 ip address 13.1.1.102 255.255.255.0
#
```

- Device F:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 120.2.0.1 255.255.255.0
#
bgp 300
 router-id 6.6.6.6
 peer 120.2.0.2 as-number 100
 #
 address-family ipv4 unicast
```

```
  network 120.2.0.0 255.255.255.0
  peer 120.2.0.2 enable
#
```

Contents

Introduction

This document introduces IGMP snooping configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the switches were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IGMP snooping.

Example: Configuring multicast group policies

Network configuration

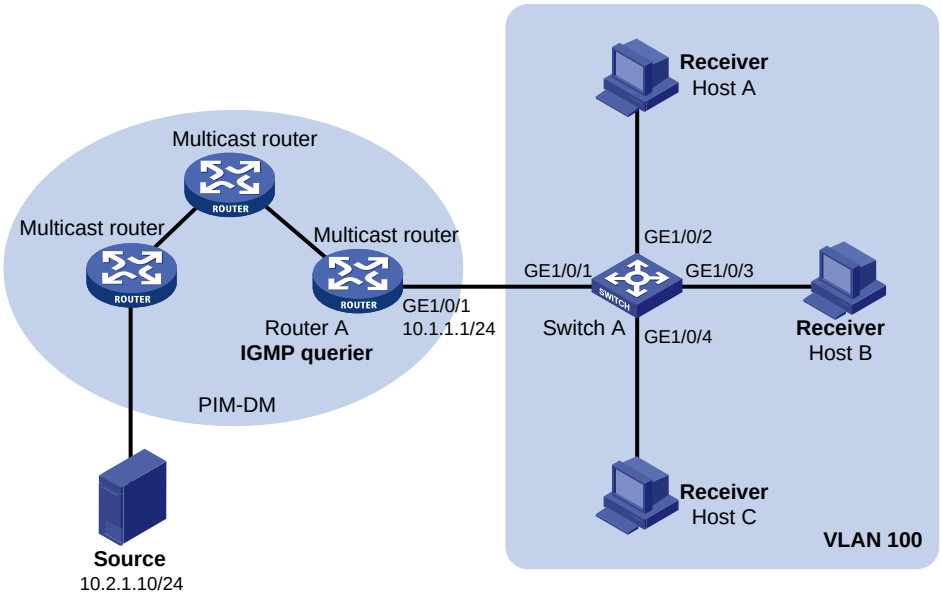
As shown in Figure 1:

- Router A runs IGMP and acts as the IGMP querier.
- Switch A runs IGMP snooping.

Configure multicast group policies on Switch A to meet the following requirements:

- Host A receives only the multicast data addressed to multicast group 224.1.1.1.
- Host B and Host C receive only the multicast data addressed to multicast group 225.1.1.1.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- IGMPv2 snooping cannot process IGMPv3 messages. It floods IGMPv3 messages in the VLAN to which the IGMPv3 messages belong. To avoid this problem, specify IGMP snooping version 3 for VLAN 100.
- To avoid receiver hosts in VLAN 100 from receiving multicast data addressed to other groups, enable dropping unknown multicast data in VLAN 100.
- To configure multicast group policies, specify a basic ACL and create ACL rules to define the groups that you want the receiver hosts to join.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure multicast group polices, follow these restrictions and guidelines:

- You must globally enable IGMP snooping in system view before you enable IGMP snooping for a VLAN in VLAN view.
- You can configure multicast group policies for all ports in IGMP-snooping view or for the current port in interface view. The configuration made in interface view takes priority over the configuration made in IGMP-snooping view.

Procedures

1. Assign an IP address and subnet mask to each interface on the routers in the PIM-DM domain. (Details not shown.)
2. Configure a unicast routing protocol on the routers in the PIM-DM domain. (Details not shown.)
3. Enable multicast routing globally on the routers in the PIM-DM domain. (Details not shown.)
4. Enable PIM-DM for the interfaces through which routers connects with each other on the routers in the PIM-DM domain. (Details not shown.)
5. Configure Router A:

   # Enable IP multicast routing globally.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   ```

   # Enable IGMPv3 on GigabitEthernet 1/0/1.

   ```
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] igmp enable
   [RouterA-GigabitEthernet1/0/1] igmp version 3
   [RouterA-GigabitEthernet1/0/1] quit
   ```

6. Configure Switch A:

   # Enable IGMP snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] igmp-snooping
   [SwitchA-igmp-snooping] quit
   ```

   # Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to VLAN 100.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
   ```

   # Enable IGMPv3 snooping and enable dropping unknown multicast data for VLAN 100.

   ```
   [SwitchA-vlan100] igmp-snooping enable
   ```

```
[SwitchA-vlan100] igmp-snooping version 3
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

Configure a multicast group policy for VLAN 100 on GigabitEthernet 1/0/2 so that Host A can join only multicast group 224.1.1.1.

```
[SwitchA] acl basic 2000
[SwitchA-acl-ipv4-basic-2000] rule permit source 224.1.1.1 0
[SwitchA-acl-ipv4-basic-2000] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] igmp-snooping group-policy 2000 vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure a multicast group policy globally for VLAN 100 so that Host B and Host C can join only multicast group 225.1.1.1.

```
[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 225.1.1.1 0
[SwitchA-acl-ipv4-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

Verifying the configuration

Send IGMP reports from Host A, Host B, and Host C to join multicast groups 224.1.1.1, 224.2.2.2, and 225.1.1.1. (Details not shown.)

Send multicast data from the source to the multicast groups. (Details not shown.)

Display dynamic IGMP snooping group entries for VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100
Total 2 entries.

VLAN 100: Total 2 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (1 in total):
      GE1/0/2                          (00:03:09)
  (0.0.0.0, 225.1.1.1)
    Host ports (2 in total):
      GE1/0/3                          (00:04:04)
      GE1/0/4                          (00:02:38)
```

The output shows the following information:

- Host A has joined multicast group 224.1.1.1 through GigabitEthernet 1/0/2, and it has not joined multicast groups 224.2.2.2 and 225.1.1.1.
- Host B and Host C have joined multicast group 225.1.1.1 through GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4, respectively. They have not joined multicast groups 224.1.1.1 and 224.2.2.2.
- Multicast group policies have taken effect.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Router A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 igmp enable
 igmp version 3
#
multicast routing
#
```

- Switch A:

```
#
igmp-snooping
 group-policy 2001 vlan 100
#
vlan 100
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping version 3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping group-policy 2000 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
acl basic 2000
 rule 0 permit source 224.1.1.1 0
#
acl basic 2001
 rule 0 permit source 225.1.1.1 0
```

#

Example: Configuring IGMP snooping static ports

Network configuration

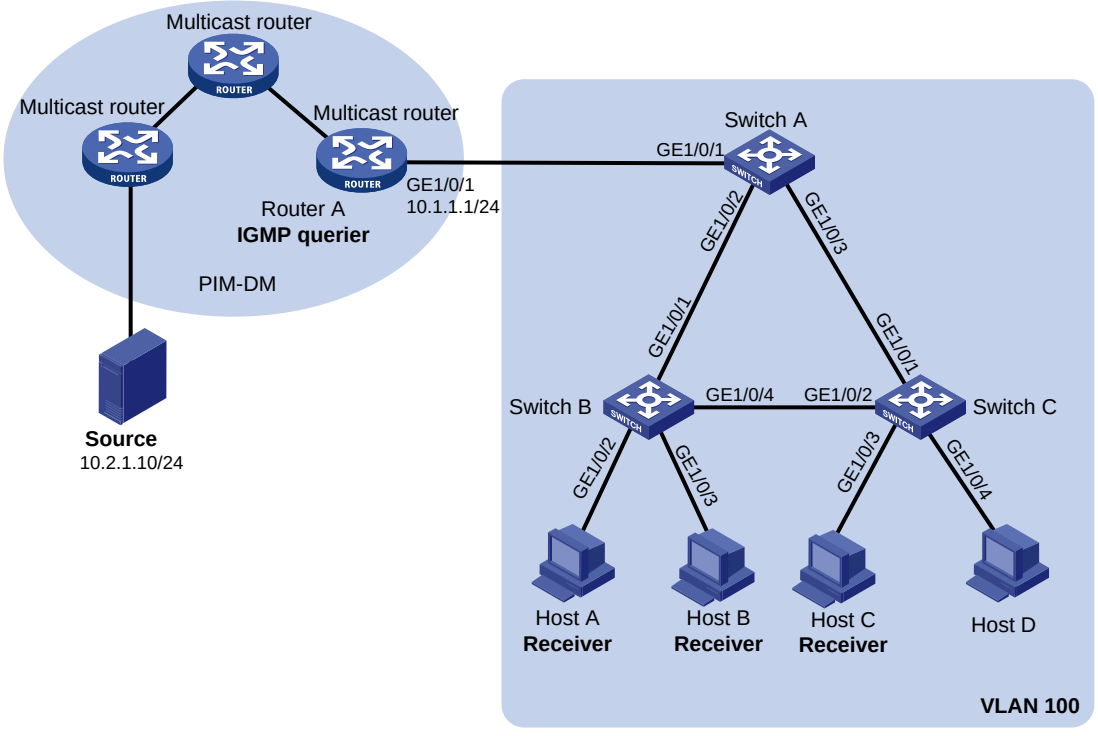
As shown in Figure 2:

- All switches in VLAN 100 run IGMP snooping.
- Router A runs IGMPv2 and acts as the IGMP querier.
- STP runs in VLAN 100. The direct route between Switch A and Switch B or the route from Switch A to Switch B with Switch C as the intermediate device is blocked to avoid loops.

Configure IGMP snooping static ports to meet the following requirements:

- Multicast data uninterruptedly flows to the receiver hosts after a link switchover occurs between Switch A and Switch B.
- Host A, Host B, and Host C permanently receive the multicast data addressed to multicast group 224.1.1.1.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- By default, when a link switchover occurs, multicast data can flow along the new link after a minimum of one IGMP query-response cycle. Multicast delivery is interrupted during this process.

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch A, GigabitEthernet 1/0/4 on Switch B, and GigabitEthernet 1/0/2 on Switch C as static router ports. Then, multicast data will be forwarded to these ports.

- Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B, and GigabitEthernet 1/0/3 on Switch C as static member ports of multicast group 224.1.1.1. Then, multicast data for the group will always be forwarded out of these ports, and Host A, Host B, and Host C can always receive the data.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series	Release 63xx

IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure IGMP snooping static ports, you must globally enable IGMP snooping in system view before you enable IGMP snooping for a VLAN in VLAN view.

Procedures

1. Assign an IP address and subnet mask to each interface on the routers in the PIM-DM domain. (Details not shown.)
2. Configure OSPF on the routers in the PIM-DM domain. (Details not shown.)
3. Enable multicast routing globally on the routers in the PIM-DM domain. (Details not shown.)
4. Enable PIM-DM for the interfaces through which routers connects with each other in the PIM-DM domain. (Details not shown.)
5. Configure Router A:

   # Enable IP multicast routing.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   ```

   # Enable IGMP on GigabitEthernet 1/0/1.

   ```
   [RouterA] interface gigabitethernet 1/0/1
   [RouterA-GigabitEthernet1/0/1] igmp enable
   [RouterA-GigabitEthernet1/0/1] quit
   ```

6. Configure Switch A:

   # Enable IGMP snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] igmp-snooping
   [SwitchA-igmp-snooping] quit
   ```

   # Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping for this VLAN.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
   [SwitchA-vlan100] igmp-snooping enable
   [SwitchA-vlan100] quit
   ```

   # Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static router ports.

   ```
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
   [SwitchA-GigabitEthernet1/0/2] quit
   [SwitchA] interface gigabitethernet 1/0/3
   [SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
   [SwitchA-GigabitEthernet1/0/3] quit
   ```

7. Configure Switch B:

   # Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping for this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/4
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Configure GigabitEthernet 1/0/4 as a static router port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] igmp-snooping static-router-port vlan 100
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static member ports for multicast group 224.1.1.1 in VLAN 100.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

8. Configure Switch C:

Enable IGMP snooping globally.

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping for this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet 1/0/2 as a static router port in VLAN 100.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] igmp-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a static member port of multicast group 224.1.1.1 in VLAN 100.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Verify the configuration before hosts join any multicast groups.

Display static router port information for VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 100:
```

```
  Router ports (2 in total):
    GE1/0/2
    GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch A have become static router ports in VLAN 100.

Display static router port information for VLAN 100 on Switch B.

```
[SwitchB] display igmp-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/4
```

The output shows that GigabitEthernet 1/0/4 on Switch B has become a static router port in VLAN 100.

Display static IGMP snooping group entries for VLAN 100 on Switch B.

```
[SwitchB] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/2
      GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B have become static member ports of multicast group 224.1.1.1 in VLAN 100.

Display static router port information for VLAN 100 on Switch C.

```
[SwitchC] display igmp-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/2
```

The output shows that GigabitEthernet 1/0/2 on Switch C has become a static router port in VLAN 100.

Display static IGMP snooping group entries for VLAN 100 on Switch C.

```
[SwitchC] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (1 in total):
      GE1/0/3
```

The output shows that GigabitEthernet 1/0/3 on Switch C has become a static group member of multicast group 224.1.1.1.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Router A:

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 igmp enable
#
multicast routing
#
```

- Switch A:

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
```

- Switch B:

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
```

```
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
```

- Switch C:

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 igmp-snooping static-group 224.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

Contents

Introduction

This document provides IGMP configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IGMP.

Example: Configuring basic IGMP features

Network configuration

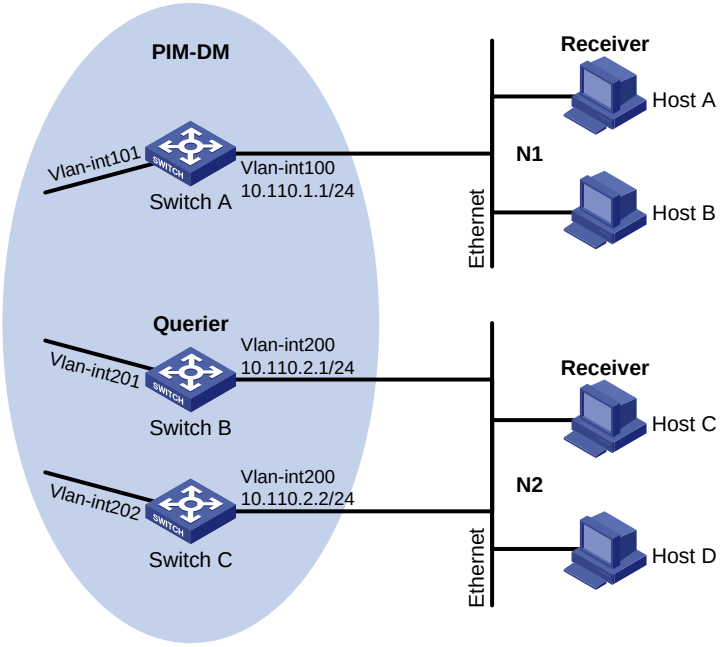
As shown in Figure 1:

- OSPF and PIM-DM run on the network.
- VOD streams are sent in multicast. Hosts of different organizations form stub networks N1 and N2.
- IGMPv2 runs between Switch A and N1, and between the other two switches and N2. Switch A acts as the IGMP querier in N1. Switch B acts as the IGMP querier in N2 because it has a lower IP address.

Configure basic IGMP features on the switches to meet the following requirements:

- Hosts in N1 can join any multicast groups.
- Hosts in N2 can join only multicast group 224.1.1.1.

Figure 1 Network diagram



Analysis

To limit the multicast groups that hosts can join, create an IPv4 basic ACL and specify the multicast groups that you want the hosts to join.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-54C switch	
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series	Not supported

S5000X-EI switch series	
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure basic IGMP features, follow these restrictions and guidelines:

- The protocol packets of different IGMP versions are different in structures and types. For IGMP to operate correctly, you must enable the same IGMP version for all switches on the same subnet.
- You must configure the same multicast group policy for all switches on the same subnet.
- By default, Ethernet interfaces, VLAN interfaces, and aggregate interfaces are shut down. You must first use the **undo shutdown** command to bring them up. This example assumes that all these interfaces are already up.

Procedures

1. Assign an IP address and subnet mask to each interface, as shown in Figure 1. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain. (Details not shown.)
3. Configure Switch A:

   # Enable IP multicast routing.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing
   [SwitchA-mrib] quit
   ```

   # Enable IGMP on the receiver-side interface VLAN-interface 100.

   ```
   [SwitchA] interface vlan-interface 100
   ```

```
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

Enable PIM-DM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

4. Configure Switch B:

Create ACL 2001 to permit IGMP reports for multicast group 224.1.1.1.

```
<SwitchB> system-view
[SwitchB] acl basic 2001
[SwitchB-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchB-acl-ipv4-basic-2001] quit
```

Enable IP multicast routing.

```
[SwitchB] multicast routing
[SwitchB-mrib] quit
```

Enable IGMP on the receiver-side interface VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
```

Configure a multicast group policy that uses ACL 2001.

```
[SwitchB-Vlan-interface200] igmp group-policy 2001
[SwitchB-Vlan-interface200] quit
```

Enable PIM-DM on VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

5. Configure Switch C:

Create ACL 2001 to permit IGMP reports for multicast group 224.1.1.1.

```
<SwitchC> system-view
[SwitchC] acl basic 2001
[SwitchC-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchC-acl-ipv4-basic-2001] quit
```

Enable IP multicast routing.

```
[SwitchC] multicast routing
[SwitchC-mrib] quit
```

Enable IGMP on the receiver-side interface VLAN-interface 200.

```
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
```

Configure a multicast group policy that uses ACL 2001.

```
[SwitchC-Vlan-interface200] igmp group-policy 2001
[SwitchC-Vlan-interface200] quit
```

Enable PIM-DM on VLAN-interface 202.

```
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

Verifying the configuration

1. Verify that hosts in N1 can join the multicast groups 224.1.1.1 and 224.1.1.2:

   # Send IGMP reports from Host A (10.110.1.10) to join the multicast groups 224.1.1.1 and 224.1.1.2. (Details not shown.)

   # Display information about IGMP groups that hosts have dynamically joined on Switch A.

```
[SwitchA] display igmp group
IGMP groups in total: 2
 Vlan-interface100 (10.110.1.1):
  IGMP groups reported in total: 2
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.1.10     00:02:04   00:01:15
   224.1.1.2       10.110.1.10     00:02:00   00:01:19
```

   The output shows that Host A has joined the multicast groups 224.1.1.1 and 224.1.1.2.

2. Verify that hosts in N2 can join only multicast group 224.1.1.1:

   # Send IGMP reports from Host C (10.110.2.10) to join the multicast groups 224.1.1.1 and 224.1.1.2. (Details not shown.)

   # Display information about IGMP groups that hosts have dynamically joined on Switch B.

```
[SwitchB] display igmp group
IGMP groups in total: 1
 Vlan-interface200(10.110.2.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.2.10     04:36:03   00:01:23
```

   # Display information about IGMP groups that hosts have dynamically joined on Switch C.

```
[SwitchC] display igmp group
IGMP groups in total: 1
 Vlan-interface200(10.110.2.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.2.10     04:21:03   00:01:13
```

   The output shows that Switch B and Switch C each have IGMP information about only the multicast group, 224.1.1.1. The multicast group policy has taken effect, and hosts in N2 can join only multicast group 224.1.1.1.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
```

```
#
interface Vlan-interface101
 ip address 10.111.1.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 101
#
multicast routing
#
```

- Switch B:

```
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200 to 201
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface201
 ip address 10.111.2.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 201
#
multicast routing
#
```

- Switch C:

```
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200
#
```

```
vlan 202
#
interface Vlan-interface200
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface202
 ip address 10.111.3.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 202
#
 multicast routing
#
```

Example: Configuring IGMP static group members

Network configuration

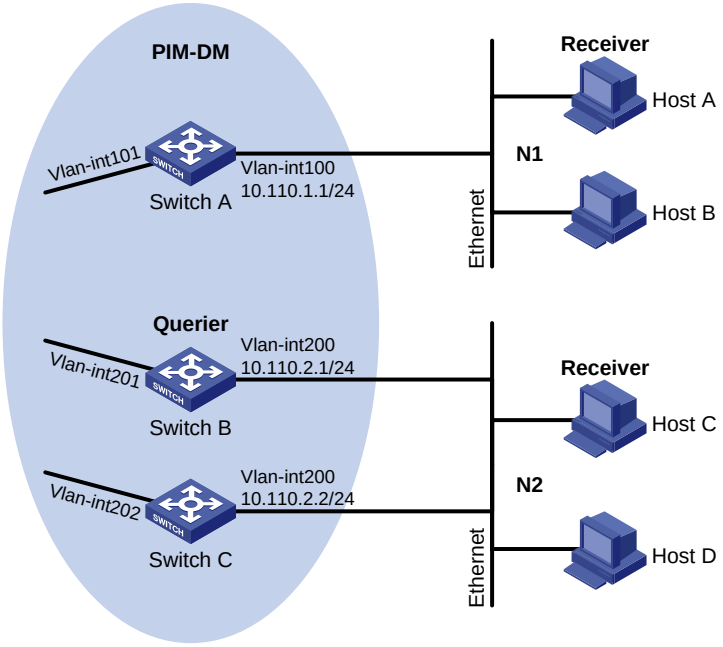
As shown in Figure 2:

- OSPF and PIM-DM run on the network.
- VOD streams are sent in multicast. Hosts of different organizations form stub networks N1 and N2.
- IGMPv2 runs between Switch A and N1, and between the other two switches and N2. Switch A acts as the IGMP querier in N1. Switch B acts as the IGMP querier in N2 because it has a lower IP address.

Configure the switches to meet the following requirements:

- Hosts in N1 can join any multicast groups, and Host A can permanently receive multicast data addressed to multicast group 224.1.1.2.
- Hosts in N2 can join only multicast group 224.1.1.1.

Figure 2 Network diagram



Analysis

For Host A to permanently receive multicast data addressed to the group 224.1.1.2, configure VLAN-interface 100 on Switch A as a static member of the multicast group.

To limit the multicast groups that hosts can join, create an IPv4 basic ACL and specify the multicast groups that you want the hosts to join.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx,

	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series	Not supported

S5000V5-EI switch series	
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure IGMP static group member ports, follow these restrictions and guidelines:

- The protocol packets of different IGMP versions are different in structures and types. For IGMP to operate correctly, specify the same IGMP version for all switches on the same subnet.
- You must configure the same multicast group policy for all switches on the same subnet.
- By default, Ethernet interfaces, VLAN interfaces, and aggregate interfaces are shut down. You must first use the **undo shutdown** command to bring them up. This example assumes that all these interfaces are already up.

Procedures

1. Assign an IP address and subnet mask to each interface, as shown in Figure 2. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain. (Details not shown.)
3. Configure Switch A:

   # Enable IP multicast routing.

   ```
   <SwitchA> system-view
   [SwitchA] multicast routing
   [SwitchA-mrib] quit
   ```

   # Enable PIM-DM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

Enable IGMP on the receiver-side interface VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
```

Configure VLAN-interface 100 as a static member of multicast group 224.1.1.2.

```
[SwitchA-Vlan-interface100] igmp static-group 224.1.1.2
[SwitchA-Vlan-interface100] quit
```

4. Configure Switch B:

Enable IP multicast routing.

```
<SwitchB> system-view
[SwitchB] multicast routing
[SwitchB-mrib] quit
```

Enable PIM-DM on VLAN-interface 201.

```
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

Create ACL 2001 to permit IGMP reports for multicast group 224.1.1.1.

```
[SwitchB] acl basic 2001
[SwitchB-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchB-acl-ipv4-basic-2001] quit
```

Enable IGMP on the receiver-side interface VLAN-interface 200.

```
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
```

Configure a multicast group policy that uses ACL 2001.

```
[SwitchB-Vlan-interface200] igmp group-policy 2001
[SwitchB-Vlan-interface200] quit
```

5. Configure Switch C:

Enable IP multicast routing.

```
<SwitchC> system-view
[SwitchC] multicast routing
[SwitchC-mrib] quit
```

Enable PIM-DM on VLAN-interface 202.

```
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

Create ACL 2001 to permit IGMP reports for multicast group 224.1.1.1.

```
[SwitchC] acl basic 2001
[SwitchC-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchC-acl-ipv4-basic-2001] quit
```

Enable IGMP on VLAN-interface 200.

```
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
```

Configure a multicast group policy that uses ACL 2001.

```
[SwitchC-Vlan-interface200] igmp group-policy 2001
[SwitchC-Vlan-interface200] quit
```

Verifying the configuration

1. Verify that hosts in N1 can join the multicast groups 224.1.1.1 and 224.1.1.2:

   # Send IGMP reports from Host A (10.110.1.10) to join the multicast groups 224.1.1.1 and 224.1.1.2. (Details not shown.)

   # Display information about IGMP groups that hosts have dynamically joined on Switch A.

```
[SwitchA] display igmp group
IGMP groups in total: 2.
 Vlan-interface100 (10.110.1.1):
  IGMP groups reported in total: 2
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.1.10     00:02:04   00:01:15
   224.1.1.2       10.110.1.10     00:02:00   00:01:19
```

   The output shows that Host A has dynamically joined the multicast groups 224.1.1.1 and 224.1.1.2.

   # Display information about IGMP groups that hosts have statically joined on Switch A.

```
[SwitchA] display igmp group static
 Entries in total: 1
   Group address   Source address  Interface         Expires
   224.1.1.2       0.0.0.0         Vlan100           Never
```

   The output shows that Host A has statically joined multicast group 224.1.1.1 through VLAN-interface 100.

2. Verify that hosts in N2 can join only multicast group 224.1.1.1:

   # Send IGMP reports from Host C (10.110.2.10) to join multicast groups 224.1.1.1 and 224.1.1.2. (Details not shown.)

   # Display information about IGMP groups that hosts have dynamically joined on Switch B.

```
[SwitchB] display igmp group
IGMP groups in total: 1
 Vlan-interface200(10.110.2.1):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.2.10     04:36:03   00:01:23
```

   # Display information about IGMP groups that hosts have dynamically joined on Switch C.

```
[SwitchC] display igmp group
IGMP groups in total: 1
 Vlan-interface200(10.110.2.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime     Expires
   224.1.1.1       10.110.2.10     04:21:03   00:01:13
```

   The output shows that Switch B and Switch C each have information only about multicast group 224.1.1.1. The multicast group policy has taken effect, and hosts in N2 can join only multicast group 224.1.1.1.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
vlan 100 to 101
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp static-group 224.1.1.2
#
interface Vlan-interface101
 ip address 10.111.1.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 101
#
multicast routing
#
```

- Switch B:

```
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200 to 201
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface201
 ip address 10.111.2.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 201
#
multicast routing
```

```
#
```

- Switch C:

```
#
acl basic 2001
 rule 0 permit source 224.1.1.1 0
#
vlan 200
#
vlan 202
#
interface Vlan-interface200
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 igmp group-policy 2001
#
interface Vlan-interface202
 ip address 10.111.3.1 255.255.255.0
 pim dm
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 202
#
 multicast routing
#
```

Example: Configuring IGMP SSM mappings

Network configuration

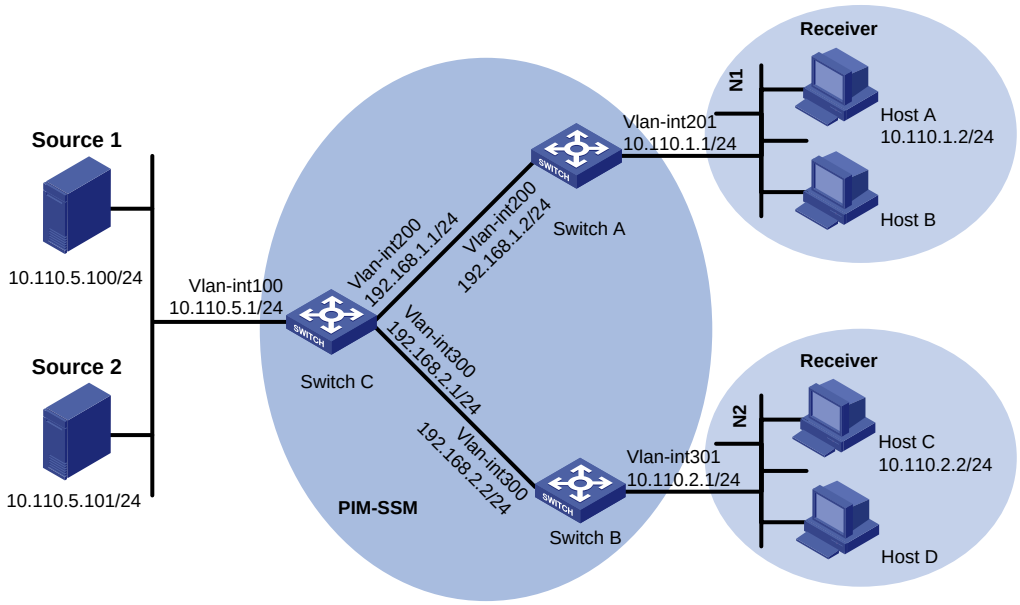
As shown in Figure 3:

- The SSM group range for the PIM-SSM domain is 232.1.1.0/24.
- Switch A and Switch B in the PIM-SSM domain run IGMPv3.
- Host A in N1 and Host B in N2 run IGMPv2, and they do not support IGMPv3. The other hosts in N1 and N2 run IGMPv3.

Configure IGMP SSM mappings on Switch A and Switch B to meet the following requirements:

- Hosts in N1 receive multicast data only from Source 1.
- Hosts in N2 receive multicast data only from Source 2.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported

MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

By default, Ethernet interfaces, VLAN interfaces, and aggregate interfaces are shut down. You must use the **undo shutdown** command to bring them up. This example assumes that all these interfaces are already up.

Procedures

1. Assign an IP address and subnet mask to each interface, as shown in Figure 3. (Details not shown.)
2. Configure OSPF on the switches in the PIM-SSM domain. (Details not shown.)
3. Enable IP multicast routing and enable PIM-SM:

   # On Switch A, enable IP multicast routing, and enable PIM-SM on VLAN-interface 200.

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] quit
```

   # Configure Switch B in the same way Switch A is configured. (Details not shown.)

   # On Router C, enable IP multicast routing, and enable PIM-SM on each interface.

```
<SwitchC> system-view
[SwitchC] multicast routing
[SwitchC-mrib] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
```

```
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] pim sm
[SwitchC-Vlan-interface300] quit
```

4. On Switch C, configure VLAN-interface 200 as a C-BSR and a C-RP:

```
[SwitchC] pim
[SwitchC-pim] c-bsr 192.168.1.1
[SwitchC-pim] c-rp 192.168.1.1
[SwitchC-pim] quit
```

5. Configure IGMPv3 on the receiver-side interfaces:

   # On Switch A, enable IGMP, and specify IGMP version 3 on VLAN-interface 201.

```
[SwitchA] interface vlan-interface201
[SwitchA-Vlan-interface201] igmp enable
[SwitchA-Vlan-interface201] igmp version 3
[SwitchA-Vlan-interface201] quit
```

   # Configure Switch B in the same way Switch A is configured. (Details not shown.)

6. Configure the SSM group range:

   # On Switch A, configure the SSM group range as 232.1.1.0/24.

```
[SwitchA] acl basic 2000
[SwitchA-acl-ipv4-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-ipv4-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

   # Configure Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

7. Configure IGMP SSM mappings:

   # On Switch A, configure an IGMP SSM mapping with multicast source 10.110.5.100 and multicast group range 232.1.1.0/24 specified in ACL 2000.

```
[SwitchA] igmp
[SwitchA-igmp] ssm-mapping 10.110.5.100 2000
[SwitchA-igmp] quit
```

   # On Switch B, configure an IGMP SSM mapping with multicast source 10.110.5.101 and multicast group range 232.1.1.0/24 specified in ACL 2000.

```
[SwitchB] igmp
[SwitchB-igmp] ssm-mapping 10.110.5.101 2000
[SwitchB-igmp] quit
```

Verifying the configuration

Send IGMPv2 reports from Host A and Host C to join multicast group 232.1.1.1. (Details not shown.)

Send multicast data from Source 1 and Source 2 to multicast group 232.1.1.1. (Details not shown.)

Display IGMP SSM mappings for multicast group 232.1.1.1 on Switch A.

```
[SwitchA] display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
```

```
 Source list:
       10.110.5.100
```

The output shows that multicast group 232.1.1.1 is associated with Source 1 (10.110.5.100). Switch A will translate (0.0.0.0, 232.1.1.1) in IGMPv2 reports to (10.110.5.100, 232.1.1.1).

Display the PIM routing table on Switch A.

```
[SwitchA] display pim routing-table
Total 0 (*, G) entries; 1 (S, G) entries

 (10.110.5.100, 232.1.1.1)
    Protocol: pim-ssm, Flag:
    UpTime: 00:13:25
    Upstream interface: Vlan-interface200
       Upstream neighbor: 192.168.1.1
       RPF prime neighbor: 192.168.1.1
    Downstream interface(s) information:
      Total number of downstreams: 1
       1: Vlan-interface201
              Protocol: igmp, UpTime: 02:54:43, Expires: 00:02:47
```

The output shows that Switch A has the (10.110.5.100, 232.1.1.1) entry.

Display IGMP SSM mappings for multicast group 232.1.1.1 on Switch B.

```
[SwitchB] display igmp ssm-mapping 232.1.1.1
 Group: 232.1.1.1
 Source list:
       10.110.5.101
```

The output shows that multicast group 232.1.1.1 is associated with Source 2 (10.110.5.101). Switch B will translate (0.0.0.0, 232.1.1.1) in IGMPv2 reports to (10.101.5.101, 232.1.1.1).

Display the PIM routing table on Switch B.

```
[SwitchB] display pim routing-table
Total 0 (*, G) entries; 1 (S, G) entries

 (10.110.5.101, 232.1.1.1)
    Protocol: pim-ssm, Flag:
    UpTime: 00:12:16
    Upstream interface: Vlan-interface300
       Upstream neighbor: 192.168.2.1
       RPF prime neighbor: 192.168.2.1
    Downstream interface(s) information:
      Total number of downstreams: 1
       1: Vlan-interface301
              Protocol: igmp, UpTime: 02:54:43, Expires: 00:02:47
```

The output shows that Switch B has the (10.110.5.101, 232.1.1.1) entry.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
interface Vlan-interface200
 pim sm
#
interface Vlan-interface201
igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl basic 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
```

- Switch B:

```
#
interface Vlan-interface300
 pim sm
#
interface Vlan-interface301
igmp enable
 igmp version 3
#
multicast routing
#
pim
 ssm-policy 2000
#
igmp
 ssm-mapping 10.110.5.100 2000
#
acl basic 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
```

- Switch C:

```
#
interface Vlan-interface100
 pim sm
#
interface Vlan-interface200
 pim sm
#
```

```
interface Vlan-interface200
 pim sm
#
multicast routing
#
pim
 c-bsr 192.168.1.1
 c-rp 192.168.1.1
#
```

Contents

Introduction

This document introduces MLD snooping configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MLD snooping.

Example: Configuring IPv6 multicast group policies

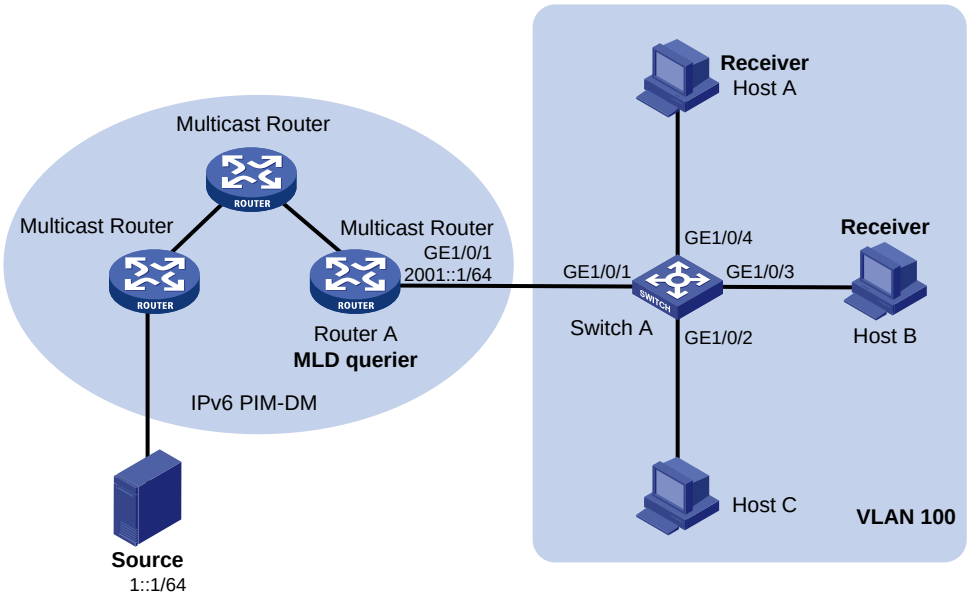
Network configuration

As shown in Figure 1:

- Router A runs MLDv1 and acts as the MLD querier in VLAN 100.
- Switch A runs MLDv1 snooping.

Configure IPv6 multicast group policies on Switch A so that Host A and Host B receive only the IPv6 multicast data addressed to IPv6 multicast group FF1E::101.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To prevent Switch A from flooding MLDv1 packets in VLAN 100, specify MLD snooping version 2 in VLAN 100. By default, MLDv1 snooping runs on the device. MLDv1 snooping processes only MLDv1 packets and floods MLDv2 packets in a VLAN.
- To prevent receiver hosts in VLAN 100 from receiving IPv6 multicast data addressed to other groups, enable dropping unknown IPv6 multicast data in VLAN 100.
- To configure an IPv6 multicast group policy, specify an IPv6 basic ACL and create ACL rules to define the groups you want the receiver hosts to join.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure IPv6 multicast group polices, follow these restrictions and guidelines:

- You must globally enable MLD snooping in system view before you enable MLD snooping for a VLAN in VLAN view.
- IPv6 multicast group filtering denies all groups if the specified ACL does not exist or the ACL does not have any rules.

Procedures

1. Assign an IPv6 address and prefix length to each interface on the routers in the IPv6 PIM-DM domain. (Details not shown.)
2. Configure an IPv6 unicast routing protocol on the routers in the IPv6 PIM-DM domain. (Details not shown.)
3. Enable IPv6 multicast routing globally on the routers in the IPv6 PIM-DM domain. (Details not shown.)
4. Enable IPv6 PIM-DM for the interfaces through which routers connects with each other on the routers in the IPv6 PIM-DM domain. (Details not shown.)
5. Configure Switch A:

   # Enable MLD snooping globally.

   ```
   <SwitchA> system-view
   [SwitchA] mld-snooping
   [SwitchA-mld-snooping] quit
   ```

   # Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN.

   ```
   [SwitchA] vlan 100
   [SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
   ```

   # In VLAN 100, enable MLD snooping, specify MLD snooping version 2, and dropping unknown IPv6 multicast data for VLAN 100.

   ```
   [SwitchA-vlan100] mld-snooping enable
   [SwitchA-vlan100] mld-snooping version 2
   [SwitchA-vlan100] mld-snooping drop-unknown
   [SwitchA-vlan100] quit
   ```

   # Configure an IPv6 multicast group policy for VLAN 100 so that receiver hosts in this VLAN can join only IPv6 multicast group FF1E::101.

   ```
   [SwitchA] acl ipv6 basic 2001
   [SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
   [SwitchA-acl-ipv6-basic-2001] quit
   ```

```
[SwitchA] mld-snooping
[SwitchA–mld-snooping] group-policy 2001 vlan 100
[SwitchA–mld-snooping] quit
```

Verifying the configuration

Send MLD reports from Host A and Host B to join IPv6 multicast groups FF1E::101 and FF1E::202. (Details not shown.)

Send IPv6 multicast data from the source to IPv6 multicast groups FF1E::101 and FF1E::202. (Details not shown.)

Display dynamic MLD snooping group entries for VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/3                                (00:03:23)
      GE1/0/4                                (00:04:10)
```

The output shows that Host A and Host B have joined IPv6 multicast group FF1E::101 through member ports GigabitEthernet 1/0/4 and GigabitEthernet 1/0/3. Host A and Host B do not join IPv6 multicast group FF1E::202. The IPv6 multicast group policy has taken effect.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

Switch A:

```
#
acl ipv6 number 2001
 rule 0 permit source FF1E::101/128
#
mld-snooping
 group-policy 2001 vlan 100
#
vlan 100
 mld-snooping enable
 mld-snooping version 2
 mld-snooping drop-unknown
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

Example: Configuring MLD snooping static ports

Network configuration

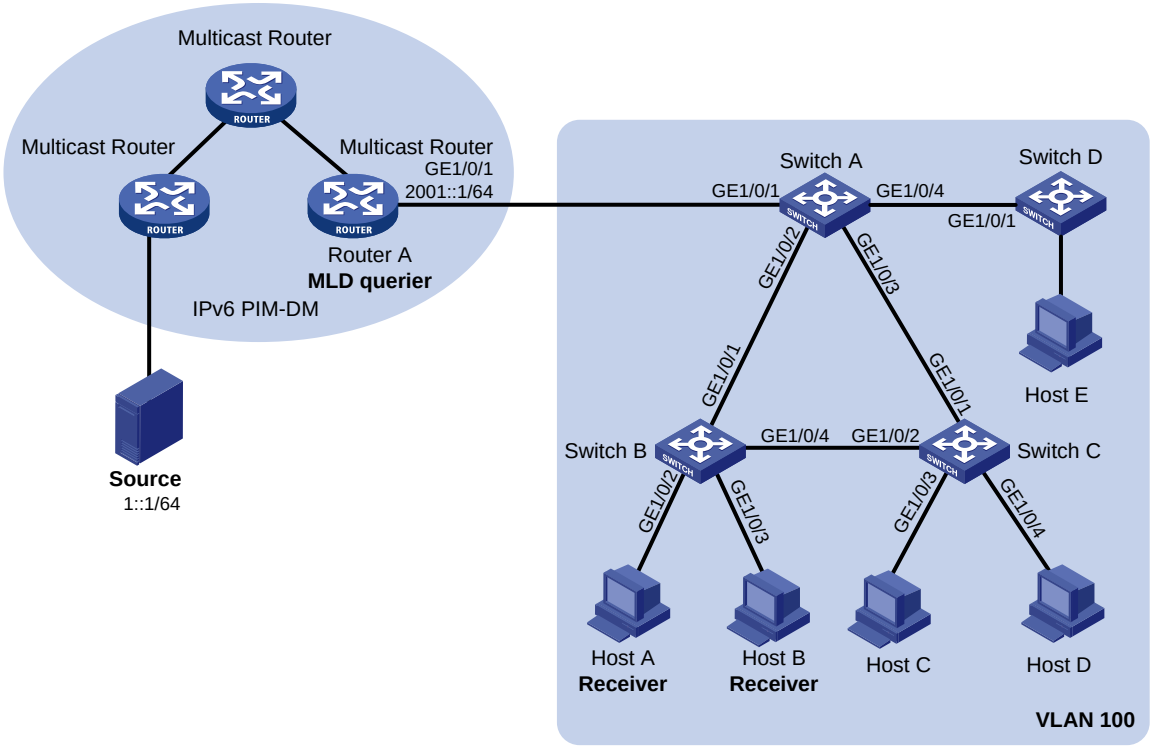
As shown in Figure 2:

- All switches in VLAN 100 run MLD snooping.
- Router A runs MLDv1 and acts as the MLD querier.
- STP runs in VLAN 100. The direct route between Switch A and Switch B or the route from Switch A to Switch B with Switch C as the intermediate device is blocked to avoid loops.

Configure MLD snooping static ports to meet the following requirements:

- IPv6 multicast data uninterruptedly flows to Host A and Host B after a link switchover occurs between Switch A and Switch B.
- Host A and Host B permanently receive the IPv6 multicast data addressed to IPv6 multicast group FF1E::101.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- By default, when a link switchover occurs, multicast data can flow along the new link after a minimum of one MLD query-response cycle. Multicast delivery is interrupted during this process.

  Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch A, GigabitEthernet 1/0/4 on Switch B, and GigabitEthernet 1/0/2 on Switch C as static router ports. Then, IPv6 multicast data will always be forwarded to these ports, and multicast delivery is uninterrupted.
- Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B as static member ports of IPv6 multicast group FF1E::101. Then, IPv6 multicast data for the group will always be forwarded out of these ports, and Host A and Host B can always receiver the data.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

You must globally enable MLD snooping in system view before you enable MLD snooping for a VLAN in VLAN view.

Procedures

1. Assign an IPv6 address and prefix length to each interface on the routers in the IPv6 PIM-DM domain. (Details not shown.)
2. Configure an IPv6 unicast routing protocol on the routers in the IPv6 PIM-DM domain. (Details not shown.)
3. Enable IPv6 multicast routing globally on the routers in the IPv6 PIM-DM domain. (Details not shown.)

4. Enable IPv6 PIM-DM for the interfaces through which routers connects with each other on the routers in the IPv6 PIM-DM domain. (Details not shown.)

5. Configure Switch A:

   # Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

   # Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable MLD snooping for this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

   # Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static router ports.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

6. Configure Switch B:

   # Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

   # Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/4 to this VLAN, and enable MLD snooping for this VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/4
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

   # Configure GigabitEthernet 1/0/4 as a static router port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] mld-snooping static-router-port vlan 100
[SwitchB-GigabitEthernet1/0/4] quit
```

   # Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as static member ports for IPv6 multicast group FF1E::101 in VLAN 100.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
```

7. Configure Switch C:

   # Enable MLD snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable MLD snooping for this VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet1/0/2 as a static router port in VLAN 100.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] mld-snooping static-router-port vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify the configuration before hosts join any multicast groups.

Display static router port information for VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router ports (2 in total):
    GE1/0/2
    GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch A have become static router ports in VLAN 100.

Display static router port information for VLAN 100 on Switch B.

```
[SwitchB] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/4
```

The output shows that GigabitEthernet 1/0/4 on Switch B has become a static router port in VLAN 100.

Display static MLD snooping group entries for VLAN 100 on Switch B.

```
[SwitchB] display mld-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (::, FF1E::101)
    Host ports (2 in total):
      GE1/0/2
      GE1/0/3
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 on Switch B have become static member ports of IPv6 multicast group FF1E::101 in VLAN 100.

Display static router port information for VLAN 100 on Switch C.

```
[SwitchC] display mld-snooping static-router-port vlan 100
VLAN 100:
  Router ports (1 in total):
    GE1/0/2
```

The output shows that GigabitEthernet 1/0/2 on Switch C has become a static router port in VLAN 100.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

- Switch B:

```
#
mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-group FF1E::101 vlan 100
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port access vlan 100
 mld-snooping static-group FF1E::101 vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
```

- Switch C:

```
#
mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mld-snooping static-router-port vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
```

Contents

Introduction

This document provides IPv6 multicast VLAN configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IPv6 multicast VLAN.

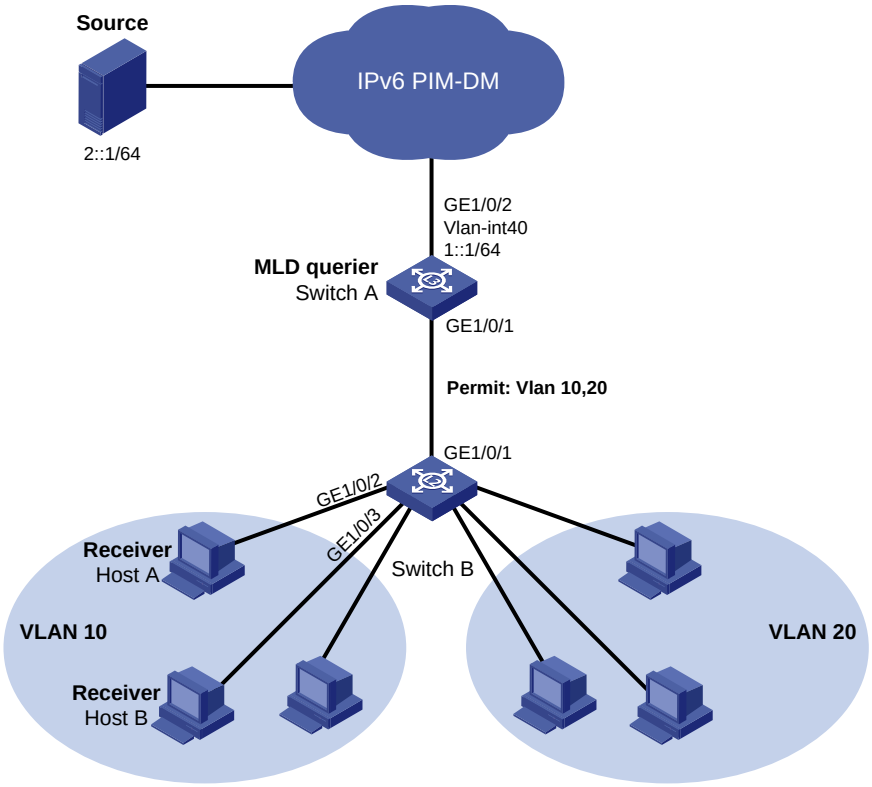
Example: Configuring sub-VLAN-based IPv6 multicast VLANs

Network configuration

As shown in Figure 1:

- VLAN 10 and VLAN 20 are Department 1 and Department 2, respectively.
- VLAN-interface 10 and VLAN-interface 20 on Layer 3 device Switch A are the gateways of VLAN 10 and VLAN 20, respectively.
- MLDv1 runs in VLAN 10 on Switch A, and MLDv1 snooping runs in VLAN 10 on Layer 2 device Switch B.
- The source sends IPv6 multicast data to IPv6 multicast group FF1E::101.
- Host A and Host B in VLAN 10 join IPv6 multicast group FF1E::101. They can receive the IPv6 multicast data that the source sends to the group.

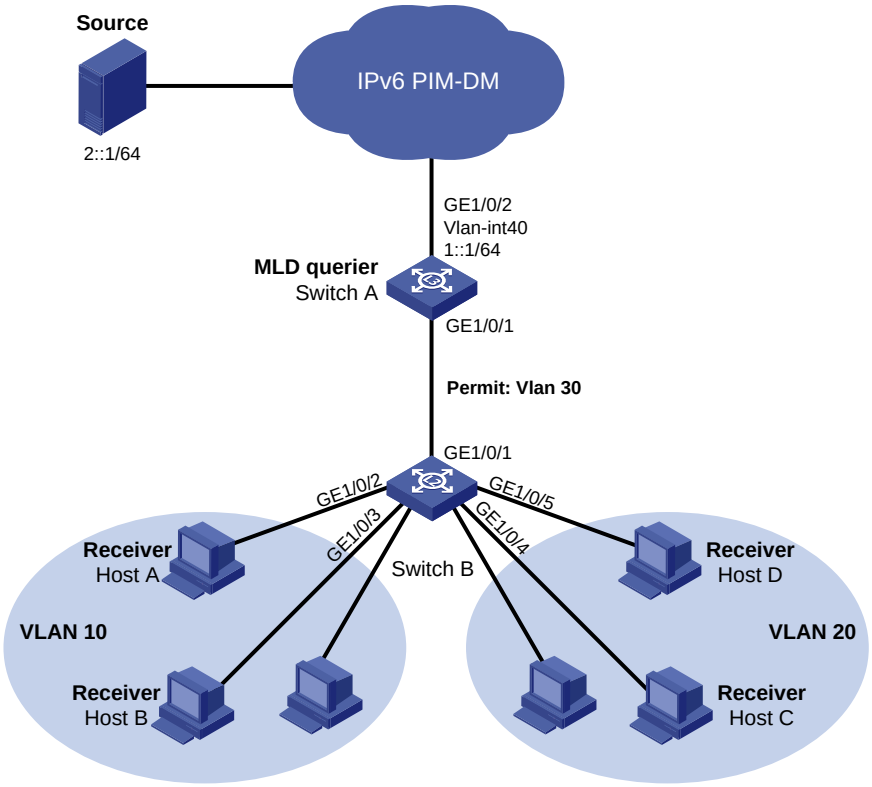
Figure 1 Network diagram



Now, Host C and Host D in VLAN 20 also join the group to receive the IPv6 multicast data, as shown in Figure 2. You can enable MLDv1 for VLAN 20 on Switch A and MLDv1 snooping for VLAN 20 on Switch B. In this way, Host C and Host D can receive the data addressed to the group. However, this occupies a large amount of bandwidth and increases the burden on Switch A.

To avoid the problems, you can configure a sub-VLAN-based IPv6 multicast VLAN on Switch B.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create VLAN 30 on Switch A and Switch B, and assign GigabitEthernet 1/0/1 on them to VLAN 30 as tagged VLAN members.
- Create VLAN-interface 30 on Switch A, and enable MLD on the interface.
- Enable MLD snooping for VLAN 10 through VLAN 30 on Switch B.
- Configure VLAN 30 on Switch B as an IPv6 multicast VLAN, and assign VLAN 10 and VLAN 20 to IPv6 multicast VLAN 30 as sub-VLANs.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx

S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx

S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure sub-VLAN-based IPv6 multicast VLANs, follow these restrictions and guidelines:

- As a best practice, do not configure IPv6 multicast VLANs on the device enabled with IPv6 multicast routing.
- The IPv6 address assigned to the VLAN interface of the IPv6 multicast VLAN must be unique on the user network.

Procedures

1. Assign IPv6 addresses to VLAN-interface 10 and VLAN-interface 20 on Switch A. (Details not shown.)

2. Configure a unicast routing protocol so that all devices on the network are interoperable at the network layer. (Details not shown.)
3. Configure Switch A:

   # Enable IPv6 multicast routing.

```
<SwitchA> system-view
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
```

   # Create VLAN 30, configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 30 as a tagged VLAN member.

```
[SwitchA] vlan 30
[SwitchA-vlan30] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 30 tagged
```

   # Create VLAN-interface 30, assign it an IPv6 address, and enable MLD on it.

```
[SwitchA] interface vlan-interface 30
[SwitchA-Vlan-interface30] ipv6 address 2001::1 64
[SwitchA-Vlan-interface30] mld enable
[SwitchA-Vlan-interface30] quit
```

   # Create VLAN 40, and assign GigabitEthernet 1/0/2 to VLAN 40.

```
[SwitchA] vlan 40
[SwitchA-vlan40] port gigabitethernet 1/0/2
[SwitchA-vlan40] quit
```

   # Create VLAN-interface 40, assign it an IPv6 address, and enable IPv6 PIM-DM on it.

```
[SwitchA] interface vlan-interface 40
[SwitchA-Vlan-interface40] ipv6 address 1::1 64
[SwitchA-Vlan-interface40] ipv6 pim dm
[SwitchA-Vlan-interface40] quit
```

4. Configure Switch B:

   # Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

   # Create VLAN 10, and enable MLD snooping for VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
```

   # Create VLAN 20, and enable MLD snooping for VLAN 20.

```
[SwitchB] vlan 20
[SwitchB-vlan20] mld-snooping enable
[SwitchB-vlan20] quit
```

   # Create VLAN 30, and enable MLD snooping for VLAN 30.

```
[SwitchB] vlan 30
[SwitchB-vlan30] mld-snooping enable
[SwitchB-vlan30] quit
```

   # Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 30 as a tagged VLAN member.

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 30 tagged
```

Configure VLAN 30 as an IPv6 multicast VLAN, and assign VLAN 10 and VLAN 20 to IPv6 multicast VLAN 30 as sub-VLANs.

```
[SwitchB] ipv6 multicast-vlan 30
[SwitchB-ipv6-mvlan-30] subvlan 10 20
[SwitchB-ipv6-mvlan-30] quit
```

Verifying the configuration

Display information about all IPv6 multicast VLANs on Switch B.

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 30:
  Sub-VLAN list(2 in total):
    10,20
  Port list(0 in total):
```

Display information about multicast groups in IPv6 multicast VLANs on Switch B.

```
[SwitchB] display ipv6 multicast-vlan group
Total 1 entries.

IPv6 multicast VLAN 30: Total 1 entries.
  (::, FF1E::101)
    Sub-VLANs (2 in total):
      VLAN 10
      VLAN 20
```

The output shows that IPv6 multicast VLAN (VLAN 30) contains sub-VLANs VLAN 10 and VLAN 20. Switch B will forward IPv6 multicast data for VLAN 30 to VLAN 10 and VLAN 20.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface Vlan-interface10
 ipv6 address 2002::1/64
```

```
#
interface Vlan-interface20
 ipv6 address 2003::1/64
#
interface Vlan-interface30
 ipv6 address 2001::1/64
 mld enable
#
interface Vlan-interface40
 ipv6 address 1::1/64
 ipv6 pim dm
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 30 tagged
 port hybrid vlan 1 untagged
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
ipv6 multicast routing
#
```

- Switch B:

```
#
mld-snooping
#
vlan 10
 mld-snooping enable
#
vlan 20
 mld-snooping enable
#
vlan 30
 mld-snooping enable
#
ipv6 multicast-vlan 30
 subvlan 10 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
port link-type hybrid
port hybrid vlan 30 tagged
port hybrid vlan 1 untagged
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 20
#
```

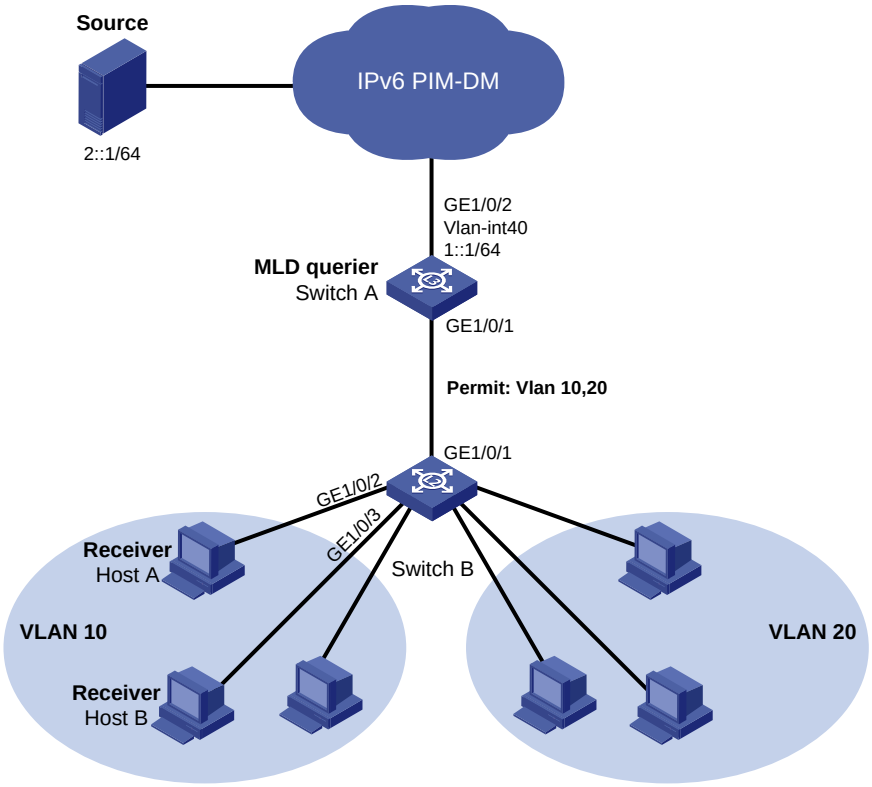
Example: Configuring port-based IPv6 multicast VLANs

Network configuration

As shown in Figure 3:

- VLAN 10 and VLAN 20 are Department 1 and Department 2, respectively.
- VLAN-interface 10 and VLAN-interface 20 on Layer 3 device Switch A are the gateways of VLAN 10 and VLAN 20, respectively.
- MLDv1 runs in VLAN 10 on Switch A, and MLDv1 snooping runs in VLAN 10 on Layer 2 device Switch B.
- The source sends IPv6 multicast data to IPv6 multicast group FF1E::101.
- Host A and Host B in VLAN 10 join IPv6 multicast group FF1E::101. They can receive the IPv6 multicast data that the source sends to the group.

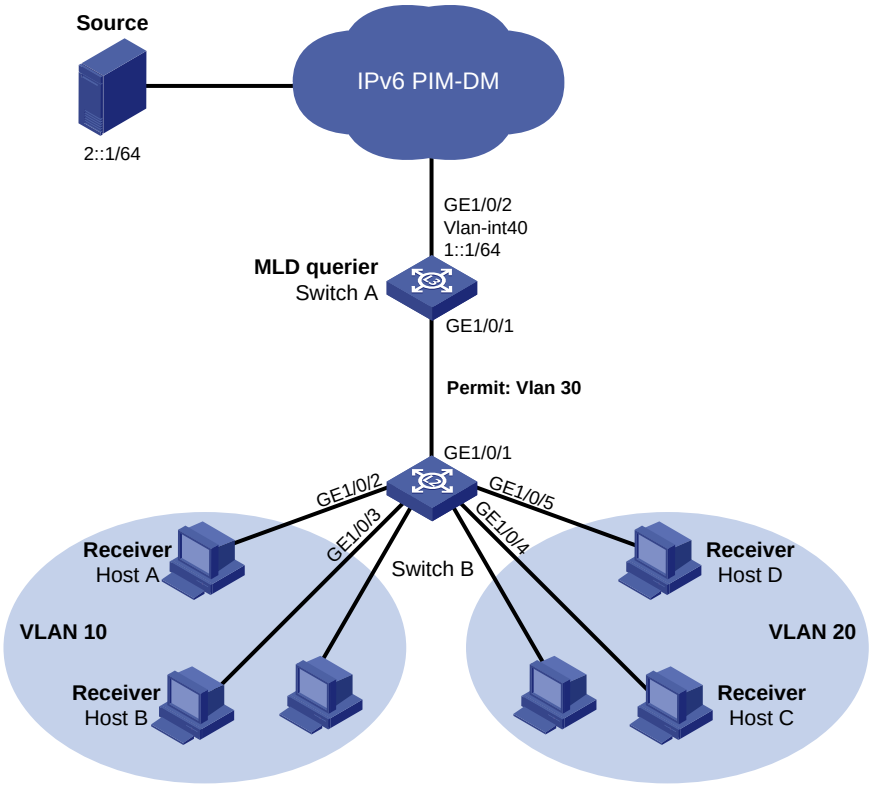
Figure 3 Network diagram



Now, Host C and Host D in VLAN 20 also join the group to receive the IPv6 multicast data, as shown in Figure 4. You can enable MLDv1 for VLAN 20 on Switch A and MLDv1 snooping for VLAN 20 on Switch B. In this way, Host C and Host D can receive the data addressed to the group. However, this occupies a large amount of bandwidth and increases the burden on Switch A.

To avoid the problems, you can configure a port-based IPv6 multicast VLAN on Switch B.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Create VLAN 30 on Switch A and Switch B, and assign GigabitEthernet 1/0/1 on them to VLAN 30 as tagged VLAN members.
- Create VLAN-interface 30 on Switch A, and enable MLD on the interface.
- On Switch B, configure the ports that have receiver hosts attached as hybrid ports, and assign the ports to their port VLAN IDs and VLAN 30 as untagged VLAN members.
- On Switch B, configure VLAN 30 as an IPv6 multicast VLAN, and assign the ports that have receiver hosts attached to IPv6 multicast VLAN 30.
- Enable MLD snooping for VLAN 10, VLAN 20, and VLAN 30 on Switch B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx

S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure port-based IPv6 multicast VLANs, follow these restrictions and guidelines:

- As a best practice, do not configure IPv6 multicast VLANs on a device enabled with IPv6 multicast routing.
- A port can belong to only one IPv6 multicast VLAN.
- The IPv6 address assigned to the VLAN interface of the IPv6 multicast VLAN must be unique on the user network.

Procedures

1. Assign IPv6 addresses to VLAN-interface 10 and VLAN-interface 20 on Switch A. (Details not shown.)
2. Configure a unicast routing protocol so that all devices on the network are interoperable at the network layer. (Details not shown.)
3. Configure Switch A:

   # Enable IPv6 multicast routing.

   ```
   <SwitchA> system-view
   [SwitchA] ipv6 multicast routing
   [SwitchA-mrib6] quit
   ```

   # Create VLAN 30, configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 30 as a tagged VLAN member.

   ```
   [SwitchA] vlan 30
   [SwitchA-vlan30] quit
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-type hybrid
   [SwitchA-GigabitEthernet1/0/1] port hybrid vlan 30 tagged
   ```

   # Create VLAN-interface 30, assign it an IPv6 address, and enable MLD on it.

   ```
   [SwitchA] interface vlan-interface 30
   [SwitchA-Vlan-interface30] ipv6 address 2001::1 64
   [SwitchA-Vlan-interface30] mld enable
   [SwitchA-Vlan-interface30] quit
   ```

   # Create VLAN 40, and assign GigabitEthernet 1/0/2 to VLAN 40.

   ```
   [SwitchA] vlan 40
   [SwitchA-vlan40] port gigabitethernet 1/0/2
   [SwitchA-vlan40] quit
   ```

   # Create VLAN-interface 40, assign it an IPv6 address, and enable IPv6 PIM-DM on it.

   ```
   [SwitchA] interface vlan-interface 40
   [SwitchA-Vlan-interface40] ipv6 address 1::1 64
   [SwitchA-Vlan-interface40] ipv6 pim dm
   [SwitchA-Vlan-interface40] quit
   ```

4. Configure Switch B:

   # Enable MLD snooping globally.

   ```
   <SwitchB> system-view
   [SwitchB] mld-snooping
   [SwitchB-mld-snooping] quit
   ```

   # Create VLAN 10, and enable MLD snooping for VLAN 10.

   ```
   [SwitchB] vlan 10
   [SwitchB-vlan10] mld-snooping enable
   [SwitchB-vlan10] quit
   ```

   # Create VLAN 20, and enable MLD snooping for VLAN 20.

   ```
   [SwitchB] vlan 20
   [SwitchB-vlan20] mld-snooping enable
   [SwitchB-vlan20] quit
   ```

   # Create VLAN 30, and enable MLD snooping for VLAN 30.

   ```
   [SwitchB] vlan 30
   ```

```
[SwitchB-vlan30] mld-snooping enable
[SwitchB-vlan30] quit
```

Configure GigabitEthernet 1/0/1 as a hybrid port, and assign it to VLAN 30 as a tagged VLAN member.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 30 tagged
```

Configure GigabitEthernet 1/0/2 as a hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
```

Set the PVID of GigabitEthernet 1/0/2 to VLAN 10, and assign the port to VLAN 10 and VLAN 30 as an untagged VLAN member.

```
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 10
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 30 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
```

Set the PVID of GigabitEthernet 1/0/3 to VLAN 10, and assign the port to VLAN 10 and VLAN 30 as an untagged VLAN member.

```
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 10
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 30 untagged
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 as a hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
```

Set the PVID of GigabitEthernet 1/0/4 to VLAN 20, and assign the port to VLAN 20 and VLAN 30 as an untagged VLAN member.

```
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 20
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 20 30 untagged
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure GigabitEthernet 1/0/5 as a hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] port link-type hybrid
```

Set the PVID of GigabitEthernet 1/0/5 to VLAN 20, and assign the port to VLAN 20 and VLAN 30 as an untagged VLAN member

```
[SwitchB-GigabitEthernet1/0/5] port hybrid pvid vlan 20
[SwitchB-GigabitEthernet1/0/5] port hybrid vlan 20 30 untagged
[SwitchB-GigabitEthernet1/0/5] quit
```

5. Configure VLAN 30 as an IPv6 multicast VLAN, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to IPv6 multicast VLAN 30.

```
[SwitchB] ipv6 multicast-vlan 30
[SwitchB-ipv6-mvlan-30] port gigabitethernet 1/0/2 to gigabitethernet 1/0/5
[SwitchB-ipv6-mvlan-30] quit
```

Verifying the configuration

Display information about IPv6 multicast VLANs on Switch B.

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.

IPv6 multicast VLAN 30:
  Sub-VLAN list(0 in total):
  Port list(4 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4
    GE1/0/5
```

Display information about dynamic MLD snooping group entries.

```
[SwitchB] display mld-snooping group
Total 1 entries.

VLAN 30: Total 1 entries.
  (::, FF1E::101)
    Host ports (4 in total):
      GE1/0/2                      (00:03:23)
      GE1/0/3                      (00:04:07)
      GE1/0/4                      (00:04:16)
      GE1/0/5                      (00:05:10)
```

The output shows that MLD snooping maintains the user ports in the multicast VLAN (VLAN 30). Switch B will forward the IPv6 multicast data of VLAN 10 through these user ports.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
ipv6 multicast-vlan 30
#
interface Vlan-interface10
 ipv6 address 2002::1/64
#
interface Vlan-interface20
 ipv6 address 2003::1/64
#
interface Vlan-interface30
```

```
 ipv6 address 2001::1/64
 mld enable
#
interface Vlan-interface40
 ipv6 address 1::1/64
 ipv6 pim dm
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 30 tagged
 port hybrid vlan 1 untagged
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
ipv6 multicast routing
#
```

- Switch B:

```
#
mld-snooping
#
vlan 10
 mld-snooping enable
#
vlan 20
 mld-snooping enable
#
vlan 30
 mld-snooping enable
#
ipv6 multicast-vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 30 tagged
 port hybrid vlan 1 untagged
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 10 30 untagged
 port hybrid pvid vlan 10
 ipv6 port multicast-vlan 30
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 10 30 untagged
 port hybrid pvid vlan 10
 ipv6 port multicast-vlan 30
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 20 30 untagged
 port hybrid pvid vlan 20
 ipv6 port multicast-vlan 30
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 20 30 untagged
 port hybrid pvid vlan 20
 ipv6 port multicast-vlan 30
#
```

Contents

Introduction

This document provides ACL configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

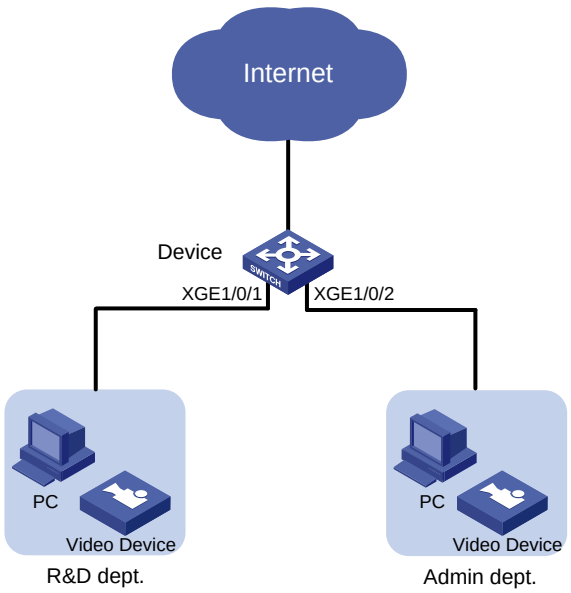
This document assumes that you have basic knowledge of ACL.

Example: Filtering packets by MAC address

Network configuration

As shown in Figure 1, the R&D department and the Administration department have video devices deployed. The video devices use MAC addresses prefixed with 000f-e2. Configure packet filtering on the device to allow outgoing video data to pass through only from 8:30 to 18:00 every day.

Figure 1 Network diagram



Analysis

Because the MAC addresses of the video devices are fixed, you can use an Ethernet frame header ACL to filter packets by MAC address. In the ACL, specify a MAC address and a mask to match the MAC addresses that have the same prefix.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series	Release 63xx

S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Procedures

Create a time range **time1** for the time range from 8:30 to 18:00 every day.

```
<Device> system-view
[Device] time-range time1 8:30 to 18:00 daily
```

Configure Ethernet frame header ACL 4000 to allow packets with source MAC addresses prefixed with 000f-e2 to pass through only during **time1**.

```
[Device] acl mac 4000
[Device-acl-mac-4000] rule permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
[Device-acl-mac-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
[Device-acl-mac-4000] quit
```

Apply ACL 4000 to filter incoming packets on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] packet-filter mac 4000 inbound
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] packet-filter mac 4000 inbound
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that the ACL is successfully applied for packet filtering.

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/1
 Inbound policy:
  MAC ACL 4000
Interface: GigabitEthernet1/0/2
 Inbound policy:
  MAC ACL 4000
```

Verify that the video devices can communicate with the external network during the time range **time1**. (Details not shown.)

Verify that the video devices cannot communicate with the external network beyond the time range **time1**. (Details not shown.)

Configuration files

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 packet-filter mac 4000 inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 packet-filter mac 4000 inbound
#
 time-range time1 08:30 to 18:00 daily
#
acl mac 4000
 rule 0 permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
 rule 5 deny source-mac 000f-e200-0000 ffff-ff00-0000
```

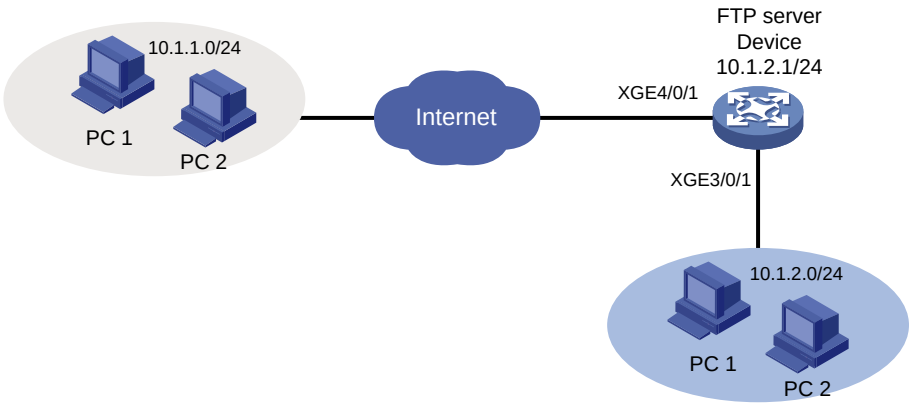
Example: Controlling FTP access

Network configuration

As shown in Figure 2, the device is an FTP server. Configure FTP access control on the device to meet the following requirements:

- Users on subnet 10.1.2.0/24 can access the FTP server at any time.
- Users on subnet 10.1.1.0/24 can access the FTP server during working hours (8:30 to 18:00) on working days (Monday to Friday).
- Qualified users are assigned the level-15 user role.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure two rules for the ACL. One rule permits packets from subnet 10.1.2.0/24. The other one permits packets from subnet 10.1.1.0/24 and takes effect only during working hours on working days.
- Use the ACL to control access to the FTP server.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch	Release 63xx

IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

Configure the time range **ftp** for working hours 8:30 to 18:00 from Monday to Friday.

```
<Device> system-view
[Device] time-range ftp 8:30 to 18:00 working-day
```

Create IPv4 basic ACL 2000.

```
[Device] acl basic 2000
```

Configure a rule to permit packets from subnet 10.1.2.0/24.

```
[Device-acl-ipv4-basic-2000] rule permit source 10.1.2.0 0.0.0.255
```

Configure a rule to permit packets from subnet 10.1.1.0/24 during the time range **ftp**.

```
[Device-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255 time-range ftp
[Device-acl-ipv4-basic-2000] quit
```

Enable FTP server on the device.

```
[Device] ftp server enable
```

Add a local user named **ftp** and authorize this user to use the FTP service.

```
[Device] local-user ftp
[Device-luser-manage-ftp] service-type ftp
```

Configure a password for the local user.

```
[Device-luser-manage-ftp] password simple 123456abcd
```

Assign the level-15 user role to the local user.

```
[Device-luser-manage-ftp] authorization-attribute user-role level-15
[Device-luser-manage-ftp] quit
```

Use the ACL 2000 to control access to the FTP server.

```
[Device] ftp server acl 2000
```

Verifying the configuration

Verify that you can use the host at 10.1.2.100 to log in to the FTP server during working hours on wording days.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
```

```
230 User logged in.
```

Verify that you can use the host at 10.1.1.100 to log in to the FTP server during working hours on working days.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

Verify that you can use the host at 10.1.2.100 to log in to the FTP server outside working hours.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

Verify that you cannot use the host at 10.1.1.100 to log in to the FTP server outside working hours.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ftp 10.1.2.1
ftp>
ftp> ls
Not connected.
```

Configuration files

```
#
 time-range ftp 08:30 to 18:00 working-day
#
acl basic 2000
 rule 0 permit source 10.1.2.0 0.0.0.255
 rule 5 permit source 10.1.1.0 0.0.0.255 time-range ftp
#
local-user ftp class manage
 password hash $h$6$SaX+pDwj5p/w/Yhq$zfUVjlVTrgH3cIRdMAZh6pXJRKcXslOXekUcSsviU7J
CP2kiv50lSL/lBU2BjnOQ2HRy7P3do7EwvxPeR/0+SA==
 service-type ftp
```

```
 authorization-attribute user-role level-15
 authorization-attribute user-role network-operator
#
 ftp server enable
 ftp server acl 2000
```

Example: Filtering packets by IP address

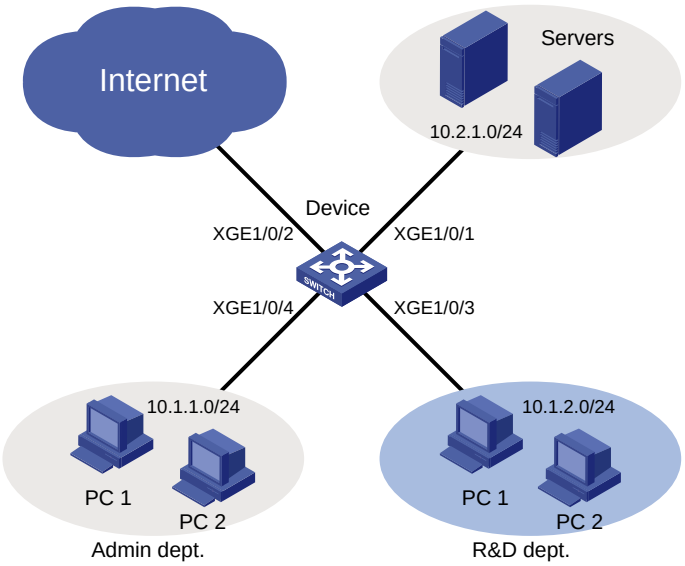
Network configuration

As shown in Figure 3, a company's internal network connects to the Internet through the device. The R&D department, Administration department, and servers are on different subnets.

Configure packet filtering to meet the following requirements:

- The Administration department can access the Internet and servers at any time, but cannot access the R&D department at any time.
- The R&D department can access only the servers during working hours (8:30 to 18:00) on working days (Monday to Friday). It can access the Internet and servers, but cannot access the Administration department outside working hours.

Figure 3 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To deny the Administration department to access the R&D department, perform the following tasks:
  - Configure an advanced ACL to deny packets destined for subnet 10.1.2.0/24.
  - Apply the ACL to filter incoming packets on GigabitEthernet 1/0/4.
- To implement access control for the R&D department, perform the following tasks:
  - Create a time range for the working hours (8:30 to 18:00) on working days (Monday to Friday).

- Create an advanced ACL and configure the following rules:
  - Configure rules to allow only packets destined for subnet 10.2.1.0/24 to pass through. Set the rules to be active during the time range.
  - To deny the R&D department to access the Administration department, configure a rule to deny packets destined for subnet 10.1.1.0/24.
- Apply the ACL to filter incoming packets on GigabitEthernet 1/0/3.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Restrictions and guidelines

When you configure ACL rules to allow the R&D department to access only the servers during working hours on working days, configure the permit rule before the deny rule. Otherwise, the interface denies all packets during working hours on working days.

Procedures

Denying the Administration department to access the R&D department

Create IPv4 advanced ACL 3000.

```
<Device> system-view
[Device] acl advanced 3000
```

Configure a rule to deny packets destined for subnet 10.1.2.0/24 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
[Device-acl-ipv4-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/4.

```
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] packet-filter 3000 inbound
[Device-GigabitEthernet1/0/4] quit
```

Configuring access control for the R&D department

Configure a time range **worktime** for the time range of 8:30 to 18:00 from Monday to Friday.

```
[Device] time-range worktime 8:30 to 18:00 working-day
```

Create IPv4 advanced ACL 3001.

```
[Device] acl advanced 3001
```

Configure a rule to allow packets destined for subnet 10.2.1.0/24 to pass through during **worktime**.

```
[Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255 time-range
worktime
```

Configure a rule to deny all IP packets to pass through during **worktime**.

```
[Device-acl-ipv4-adv-3001] rule deny ip time-range worktime
```

Configure a rule to deny packets destined for subnet 10.1.1.0/24 to pass through.

```
[Device-acl-ipv4-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255
[Device-acl-ipv4-adv-3001] quit
```

Apply ACL 3001 to filter incoming packets on GigabitEthernet 1/0/3.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3001 inbound
[Device-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Verify that the ACLs are successfully applied for packet filtering.

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/3
 Inbound policy:
  IPv4 ACL 3001
Interface: GigabitEthernet1/0/4
 Inbound policy:
  IPv4 ACL 3000
```

Verify that you cannot ping through a website on the Internet from the R&D department at 9:30 on Monday.

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Verify that you can ping through a website on the Internet from the Administration department at 9:30 on Monday.

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:
```

```
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

Verify that you can ping through a website on the Internet from the R&D department at 19:30 on Monday.

```
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

Configuration files

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 packet-filter 3001 inbound
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 packet-filter 3000 inbound
#
 time-range worktime 08:30 to 18:00 working-day
#
acl advanced 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip destination 10.2.1.0 0.0.0.255 time-range worktime
 rule 5 deny ip time-range worktime
```

```
rule 10 deny ip destination 10.1.1.0 0.0.0.255
```

Example: Filtering TCP packets

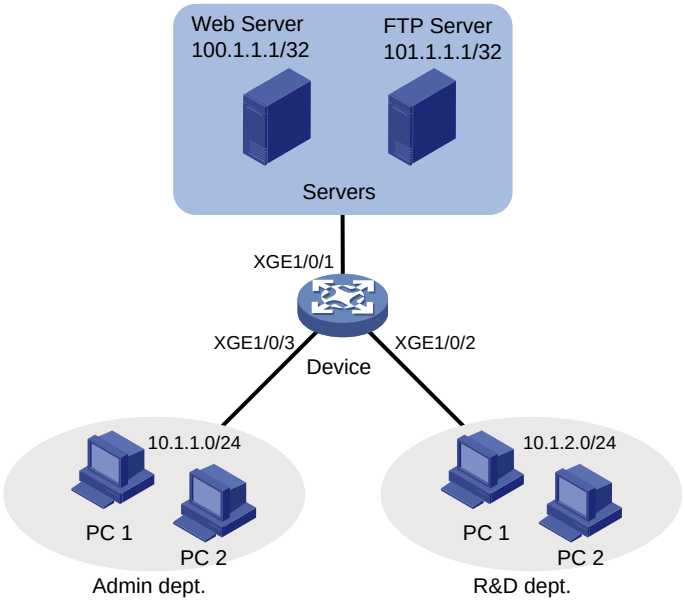
Network configuration

As shown in Figure 4, the R&D department, Administration department, and servers are on different networks, and they are connected through the device.

Configure packet filtering to meet the following requirements:

- The Web server provides HTTP services to only the Administration department.
- The FTP server provides FTP services to only the R&D department.
- The TCP connections between hosts and the Web server can only be initiated by the hosts. The TCP connections between hosts and the FTP server can be initiated by either the hosts or the FTP server.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To allow TCP connections initiated by the hosts to the Web server, perform the following tasks:
  - Configure an advanced ACL rule as follows to allow packets sent by the Web server through established TCP connections to pass through:
    - Specify the **established** keyword (the ACK or RST flag bit set) in the rule to match established TCP connections.
    - Because a TCP initiator typically uses a TCP port number higher than 1023, specify a port number range higher than 1023 to match established TCP connections.
  - Configure an advanced ACL rule to deny packets sent from the subnet where the Web server resides to the subnet where the hosts reside.

- FTP uses TCP port 20 for data transfer and port 21 for FTP control. To identify FTP traffic, you must specify TCP ports 20 and 21 in ACL rules.
- To identify HTTP packets, specify TCP port 80 in ACL rules.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx

S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx

S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Procedures

Configuring access control for the Administration department

Create IPv4 advanced ACL 3000.

```
<Device> system-view
[Device] acl advanced 3000
```

Configure a rule to allow TCP packets from the Web server to the hosts on subnet 10.1.1.0/24, with TCP port number higher than 1023 and the ACK or RST flag set.

```
[Device-acl-ipv4-adv-3000] rule permit tcp established source 100.1.1.1 0 destination
10.1.1.0 0.0.0.255 destination-port gt 1023
```

Configure a rule to deny TCP packets from subnet 100.1.1.1/32 to subnet 10.1.1.0/24 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 100.1.1.1 0 destination 10.1.1.0
0.0.0.255
```

Configure a rule to deny FTP packets sourced from 101.1.1.1/32 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 101.1.1.1 0 source-port range 20 21
[Device-acl-ipv4-adv-3000] quit
```

Apply ACL 3000 to filter outgoing packets on GigabitEthernet 1/0/3.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3000 outbound
[Device-GigabitEthernet1/0/3] quit
```

Configuring access control for the R&D department

Create IPv4 advanced ACL 3001.

```
[Device] acl advanced 3001
```

Configure a rule to deny HTTP packets sourced from 100.1.1.1/32 to pass through.

```
[Device-acl-ipv4-adv-3001] rule deny tcp source 100.1.1.1 0 source-port eq 80
[Device-acl-ipv4-adv-3001] quit
```

Apply ACL 3001 to filter outgoing packets on GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] packet-filter 3001 outbound
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify that the ACLs are successfully applied for packet filtering.

   ```
   [Device] display packet-filter interface outbound
   Interface: GigabitEthernet1/0/2
    Outbound policy:
     IPv4 ACL 3001
   Interface: GigabitEthernet1/0/3
    Outbound policy:
     IPv4 ACL 3000
   ```

2. Verify that you cannot Telnet to the FTP server from the Administration department.

   ```
   C:\>telnet 101.1.1.1 21
   Connecting To 101.1.1.1...Could not open connection to the host, on port 21:
    Connect failed

   C:\>
   ```

3. Verify that from the Web server, you can ping a host in the Administration department, but cannot access a shared folder on the host:

   # Set a shared folder on a host in the Administration department. (Details not shown.)

   # Ping the host from the Web server. The ping operation succeeds.

   ```
   C:\>ping 10.1.1.110

   Pinging 10.1.1.110 with 32 bytes of data:
   Reply from 10.1.1.110: bytes=32 time=2ms TTL=128
   Reply from 10.1.1.110: bytes=32 time=14ms TTL=128
   Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
   Reply from 10.1.1.110: bytes=32 time=1ms TTL=128

   Ping statistics for 10.1.1.110:
       Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
       Minimum = 1ms, Maximum = 14ms, Average = 4ms

   C:\>
   ```

   # Verify that you cannot access the share folder from the Web server. (Details not shown.)

4. Verify that you cannot Telnet to the Web server from the R&D department.

   ```
   C:\>telnet 100.1.1.1 80
   Connecting To 100.1.1.1...Could not open connection to the host, on port 80:
    Connect failed
   ```

```
C:\>
```

Configuration files

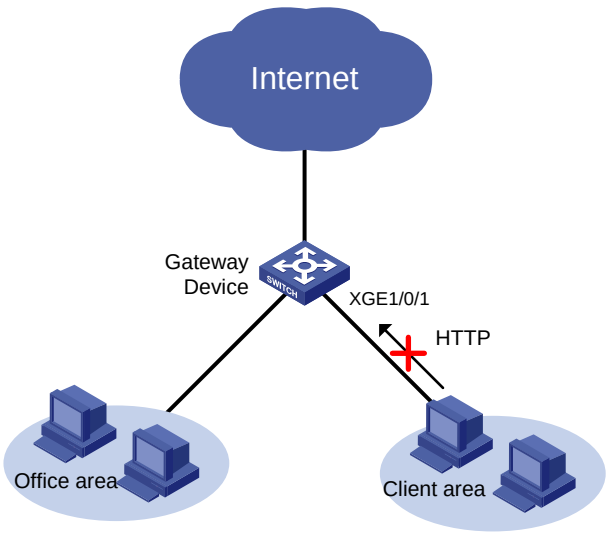
```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 packet-filter 3001 outbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 packet-filter 3000 outbound
#
acl advanced 3000
 rule 0 permit tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination
-port gt 1023 established
 rule 5 deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255
 rule 10 deny tcp source 101.1.1.1 0 source-port range ftp-data ftp
#
acl advanced 3001
 rule 0 deny tcp source 100.1.1.1 0 source-port eq www
```

Example: Filtering HTTP packets by using a user-defined ACL

Network configuration

As shown in Figure 5, configure a used-defined ACL on the device to discard HTTP packets from all clients in the client area.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported

S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Procedures

Create user-defined ACL 5000.

```
<Device> system-view
```

```
[Device] acl user-defined 5000
```

Configure a rule to deny HTTP packets.

```
[Device-acl-user-5000] rule deny l4 1f90 ffff 0
[Device-acl-user-5000] quit
```

Apply ACL 3000 to filter incoming packets on Ten-GigabitEthernet 1/0/1.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] packet-filter user-defined 5000 inbound
[Device-Ten-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that the ACL is successfully applied for packet filtering.

```
[Device] display packet-filter interface inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  User-defined ACL 5000
```

Configuration files

```
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 packet-filter user-defined 5000 inbound
#
acl user-defined 5000
 rule 0 deny l4 1f90 ffff 0
```

Contents

Introduction

This chapter provides examples for configuring traffic policing and aggregate CAR to control network traffic.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of traffic policing.

Example: Policing traffic by IP address and protocol type

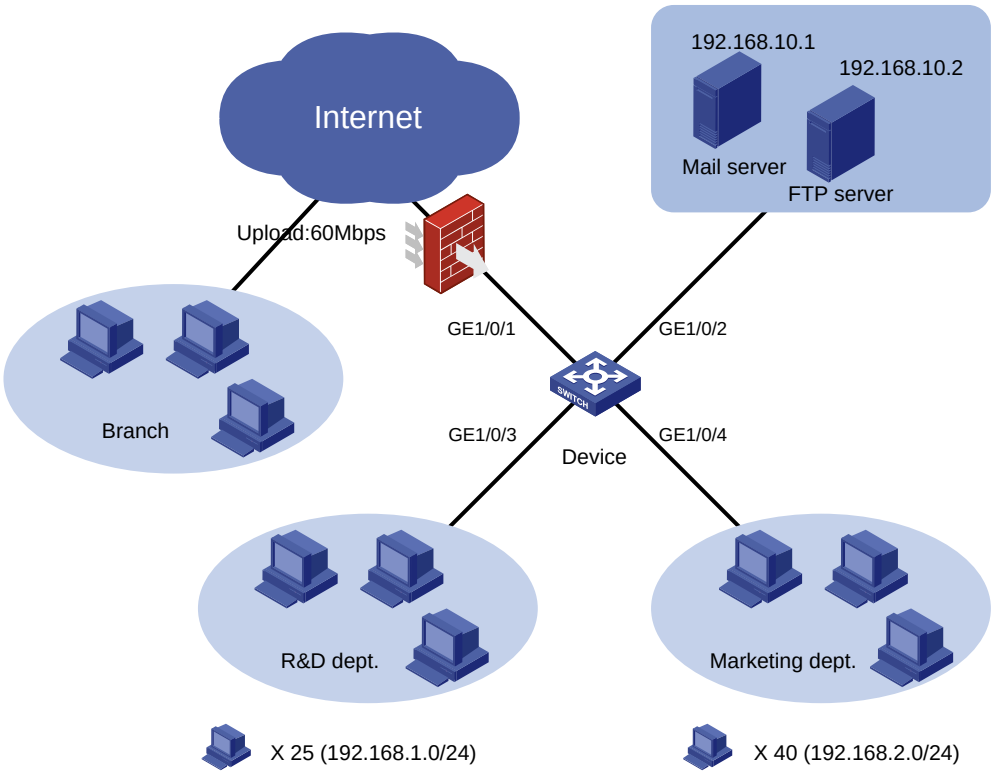
Network configuration

As shown in Figure 1, a company uses a dedicated line to access the Internet, with an uplink bandwidth of 60 Mbps. All end devices use the firewall as the gateway. The mail server forwards emails for all clients to the external network. The FTP server provides data services for the branch through the Internet.

Configure traffic policing to classify and rate limit the uplink traffic as follows:

- **HTTP traffic**—Rate limit HTTP traffic to a total rate of 40 Mbps (15 Mbps for the 25 hosts in the R&D department and 25 Mbps for the 40 hosts in the Marketing department).
- **Email traffic**—Rate limit email traffic to 2 Mbps.
- **FTP traffic**—Rate limit FTP traffic to 10 Mbps.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure ACLs to classify packets of different types.
- Associate classes with policing actions to rate limit packets of different types.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx

S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Procedures

1. Police HTTP traffic from the R&D department:

Create advanced IPv4 ACL 3000 to match HTTP traffic from the R&D department.

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80 source
192.168.1.0 0.0.0.255
[Device-acl-ipv4-adv-3000] quit
```

Create a class named **rd_http**, and use advanced IPv4 ACL 3000 as the match criterion.

```
[Device] traffic classifier rd_http
[Device-classifier-rd_http] if-match acl 3000
[Device-classifier-rd_http] quit
```

Create a behavior named **rd_http**, and configure traffic policing with the CIR of 15 Mbps.

```
[Device] traffic behavior rd_http
[Device-behavior-rd_http] car cir 15360
[Device-behavior-rd_http] quit
```

Create a QoS policy named **rd_http**, and associate the class **rd_http** with the behavior **rd_http** in the QoS policy.

```
[Device] qos policy rd_http
[Device-qospolicy-rd_http] classifier rd_http behavior rd_http
[Device-qospolicy-rd_http] quit
```

Apply the QoS policy **rd_http** to the inbound direction of interface GigabitEthernet 1/0/3.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy rd_http inbound
[Device-GigabitEthernet1/0/3] quit
```

2. Police HTTP traffic from the Marketing department:

Create advanced IPv4 ACL 3001 to match HTTP traffic from the Marketing department.

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule permit tcp destination-port eq 80 source
192.168.2.0 0.0.0.255
[Device-acl-ipv4-adv-3001] quit
```

Create a class named **mkt_http**, and use advanced IPv4 ACL 3001 as the match criterion.

```
[Device] traffic classifier mkt_http
[Device-classifier-mkt_http] if-match acl 3001
[Device-classifier-mkt_http] quit
```

Create a behavior named **mkt_http**, and configure traffic policing with the CIR of 25 Mbps.

```
[Device] traffic behavior mkt_http
[Device-behavior-mkt_http] car cir 25600
[Device-behavior-mkt_http] quit
```

Create a QoS policy named **mkt_http**, and associate the class **mkt_http** with the behavior **mkt_http** in the QoS policy.

```
[Device] qos policy mkt_http
[Device-qospolicy-mkt_http] classifier mkt_http behavior mkt_http
[Device-qospolicy-mkt_http] quit
```

Apply the QoS policy **mkt_http** to the inbound direction of interface GigabitEthernet 1/0/4.

```
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] qos apply policy mkt_http inbound
[Device-GigabitEthernet1/0/4] quit
```

3. Police email traffic and FTP traffic:

Create advanced IPv4 ACL 3002 to match email traffic.

```
[Device] acl advanced 3002
```

```
[Device-acl-ipv4-adv-3002] rule permit tcp destination-port eq smtp source
192.168.10.1 0.0.0.0
[Device-acl-ipv4-adv-3002] quit
```

Create a class named **email**, and use advanced IPv4 ACL 3002 as the match criterion.

```
[Device] traffic classifier email
[Device-classifier-email] if-match acl 3002
[Device-classifier-email] quit
```

Create a behavior named **email**, and configure traffic policing with the CIR of 2 Mbps.

```
[Device] traffic behavior email
[Device-behavior-email] car cir 2048
[Device-behavior-email] quit
```

Create basic IPv4 ACL 2001 to match FTP traffic.

```
[Device] acl basic 2001
[Device-acl-ipv4-basic-2001] rule permit source 192.168.10.2 0.0.0.0
[Device-acl-ipv4-basic-2001] quit
```

Create a class named **ftp**, and use basic IPv4 ACL 2001 as the match criterion.

```
[Device] traffic classifier ftp
[Device-classifier-ftp] if-match acl 2001
[Device-classifier-ftp] quit
```

Create a behavior named **ftp**, and configure traffic policing with the CIR of 10 Mbps.

```
[Device] traffic behavior ftp
[Device-behavior-ftp] car cir 10240
[Device-behavior-ftp] quit
```

Create a QoS policy named **email&ftp**, and associate the classes **email** and **ftp** with the behavior **email** and **ftp** in the QoS policy, respectively.

```
[Device] qos policy email&ftp
[Device-qospolicy-email&ftp] classifier email behavior email
[Device-qospolicy-email&ftp] classifier ftp behavior ftp
[Device-qospolicy-email&ftp] quit
```

Apply the QoS policy **email&ftp** to the inbound direction of interface GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy email&ftp inbound
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify QoS policies applied to interfaces.

```
[Device] display qos policy interface
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: email&ftp
   Classifier: email
     Operator: AND
     Rule(s) :
      If-match acl 3002
     Behavior: email
      Committed Access Rate:
        CIR 2048 (kbps), CBS 128000 (Bytes), EBS 0 (Bytes)
```

```
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: ftp
     Operator: AND
     Rule(s) :
      If-match acl 2001
     Behavior: ftp
      Committed Access Rate:
        CIR 10240 (kbps), CBS 640000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/3
  Direction: Inbound
  Policy: rd_http
   Classifier: rd_http
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: rd_http
      Committed Access Rate:
        CIR 15360 (kbps), CBS 960000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet1/0/4
  Direction: Inbound
  Policy: mkt_http
   Classifier: mkt_http
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: mkt_http
      Committed Access Rate:
        CIR 25600 (kbps), CBS 1600000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
```

```
        Red packets   : 0 (Packets)
```

Configuration files

```
#
traffic classifier email operator and
 if-match acl 3002
#
traffic classifier ftp operator and
 if-match acl 2001
#
traffic classifier mkt_http operator and
 if-match acl 3001
#
traffic classifier rd_http operator and
 if-match acl 3000
#
traffic behavior email
 car cir 2048 cbs 128000 ebs 0 green pass red discard yellow pass
#
traffic behavior ftp
 car cir 10240 cbs 640000 ebs 0 green pass red discard yellow pass
#
traffic behavior mkt_http
 car cir 25600 cbs 1600000 ebs 0 green pass red discard yellow pass
#
traffic behavior rd_http
 car cir 15360 cbs 960000 ebs 0 green pass red discard yellow pass
#
qos policy email&ftp
 classifier email behavior email
 classifier ftp behavior ftp
#
qos policy mkt_http
 classifier mkt_http behavior mkt_http
#
qos policy rd_http
 classifier rd_http behavior rd_http
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos apply policy email&ftp inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy rd_http inbound
#
interface GigabitEthernet1/0/4
```

```
 port link-mode bridge
 qos apply policy mkt_http inbound
#
acl basic 2001
 rule 0 permit source 192.168.10.2 0
#
acl advanced 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq www
#
acl advanced 3001
 rule 0 permit tcp source 192.168.2.0 0.0.0.255 destination-port eq www
#
acl advanced 3002
 rule 0 permit tcp source 192.168.10.1 0 destination-port eq smtp
```

Example: Allocating bandwidth based on VLANs

Network configuration

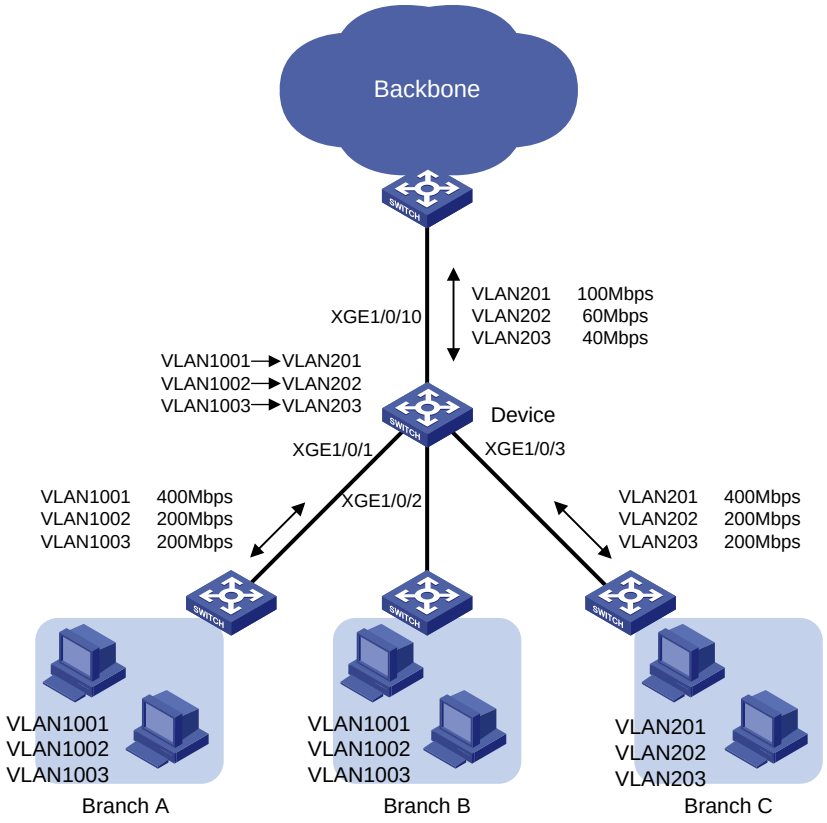
As shown in Figure 2, the device aggregates traffic from the branches and transmits the traffic to the backbone network through a leased line. Each branch site assigns packets of different applications to different VLANs.

- Configure one-to-one VLAN mapping on the following interfaces of the device to re-map traffic of different applications to VLANs as per the transmission scheme on the backbone network:
  - GigabitEthernet 1/0/1.
  - GigabitEthernet 1/0/2.
- Configure traffic policing to allocate bandwidth to traffic from different VLANs, as shown in Table 1.

Table 1 Bandwidth allocation

XGE 1/0/1 and XGE 1/0/2 (uplink or downlink)			**XGE 1/0/3 (uplink or downlink)**			**XGE 1/0/10 (uplink or downlink)**		
VLAN 1001	VLAN 1002	VLAN 1003	VLAN 201	VLAN 202	VLAN 203	VLAN 201	VLAN 202	VLAN 203
400 Mbps	200 Mbps	200 Mbps	400 Mbps	200 Mbps	200 Mbps	100 Mbps	60 Mbps	40 Mbps

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure VLAN-based traffic classes.
- Configure per-VLAN traffic policing behaviors.
- Associate each class with its specific traffic behavior.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported

S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

Configuring VLAN settings

1. Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as follows:
   - Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports.
   - Assign them to VLANs 1001 through 1003 and VLANs 201 through 203.
   - Remove them from VLAN 1.
   - Configure one-to-one VLAN mappings on the two interfaces.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
[Device-GigabitEthernet1/0/1] port trunk permit vlan 1001 to 1003 201 to 203
[Device-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/1] vlan mapping 1001 translated-vlan 201
[Device-GigabitEthernet1/0/1] vlan mapping 1002 translated-vlan 202
[Device-GigabitEthernet1/0/1] vlan mapping 1003 translated-vlan 203
```

```
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-type trunk
[Device-GigabitEthernet1/0/2] port trunk permit vlan 1001 to 1003 201 to 203
[Device-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/2] vlan mapping 1001 translated-vlan 201
[Device-GigabitEthernet1/0/2] vlan mapping 1002 translated-vlan 202
[Device-GigabitEthernet1/0/2] vlan mapping 1003 translated-vlan 203
[Device-GigabitEthernet1/0/2] quit
```

2. Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/10 as follows:
   - Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/10 as trunk ports.
   - Assign them to VLANs 201 through 203.
   - Remove them from VLAN 1.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port link-type trunk
[Device-GigabitEthernet1/0/3] port trunk permit vlan 201 to 203
[Device-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/3] quit
[Device] interface gigabitethernet 1/0/10
[Device-GigabitEthernet1/0/10] port link-type trunk
[Device-GigabitEthernet1/0/10] port trunk permit vlan 201 to 203
[Device-GigabitEthernet1/0/10] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/10] quit
```

Configuring traffic policing

1. Configure traffic policing for the traffic from and to branches:

Create a class named **vlan201**, and configure CVLAN 201 as the match criterion.

```
[Device-classifier-vlan201] if-match customer-vlan-id 201
[Device-classifier-vlan201] quit
```

Create a class named **vlan202**, and configure CVLAN 202 as the match criterion.

```
[Device] traffic classifier vlan202
[Device-classifier-vlan202] if-match customer-vlan-id 202
[Device-classifier-vlan202] quit
```

Create a class named **vlan203**, and configure CVLAN 203 as the match criterion.

```
[Device] traffic classifier vlan203
[Device-classifier-vlan203] if-match customer-vlan-id 203
[Device-classifier-vlan203] quit
```

Create a behavior named **car400**, and configure a CIR of 400 Mbps.

```
[Device] traffic behavior car400
[Device-behavior-car400] car cir 409600
[Device-behavior-car400] quit
```

Create a behavior named **car200**, and configure a CIR of 200 Mbps.

```
[Device] traffic behavior car200
[Device-behavior-car200] car cir 204800
[Device-behavior-car200] quit
```

Create a QoS policy named **ABCupdown**, and associate the classes with the behaviors.

```
[Device] qos policy ABCupdown
[Device-qospolicy-ABCupdown] classifier vlan201 behavior car400
[Device-qospolicy-ABCupdown] classifier vlan202 behavior car200
[Device-qospolicy-ABCupdown] classifier vlan203 behavior car200
[Device-qospolicy-ABCupdown] quit
```

Apply the QoS policy to both directions of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy ABCupdown inbound
[Device-GigabitEthernet1/0/1] qos apply policy ABCupdown outbound
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy ABCupdown inbound
[Device-GigabitEthernet1/0/2] qos apply policy ABCupdown outbound
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy ABCupdown inbound
[Device-GigabitEthernet1/0/3] qos apply policy ABCupdown outbound
[Device-GigabitEthernet1/0/3] quit
```

2. Configure traffic policing for the traffic from and to the backbone network:

Create a behavior named **car100**, and configure a CIR of 100 Mbps.

```
[Device] traffic behavior car100
[Device-behavior-car100] car cir 102400
[Device-behavior-car100] quit
```

Create a behavior named **car60**, and configure a CIR of 60 Mbps.

```
[Device] traffic behavior car60
[Device-behavior-car60] car cir 61440
[Device-behavior-car60] quit
```

Create a behavior named **car40**, and configure a CIR of 40 Mbps.

```
[Device] traffic behavior car40
[Device-behavior-car40] car cir 40960
[Device-behavior-car40] quit
```

Create a QoS policy named **BONEupdown**, and associate the classes with the behaviors.

```
[Device] qos policy BONEupdown
[Device-qospolicy-BONEupdown] classifier vlan201 behavior car100
[Device-qospolicy-BONEupdown] classifier vlan202 behavior car60
[Device-qospolicy-BONEupdown] classifier vlan203 behavior car40
[Device-qospolicy-BONEupdown] quit
```

Apply the QoS policy to both directions of GigabitEthernet 1/0/10.

```
[Device] interface gigabitethernet 1/0/10
[Device-GigabitEthernet1/0/10] qos apply policy BONEupdown inbound
[Device-GigabitEthernet1/0/10] qos apply policy BONEupdown outbound
[Device-GigabitEthernet1/0/10] quit
```

Figure 3 shows how the switches process the uplink traffic from a branch to the backbone network. The figure uses VLAN 1001 as an example.

Figure 3 Uplink traffic processing

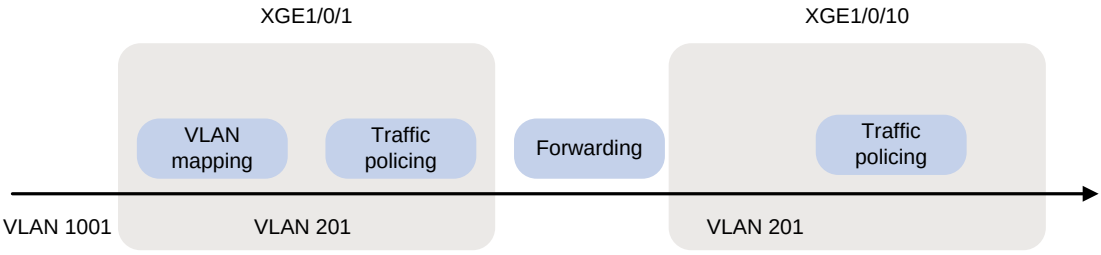
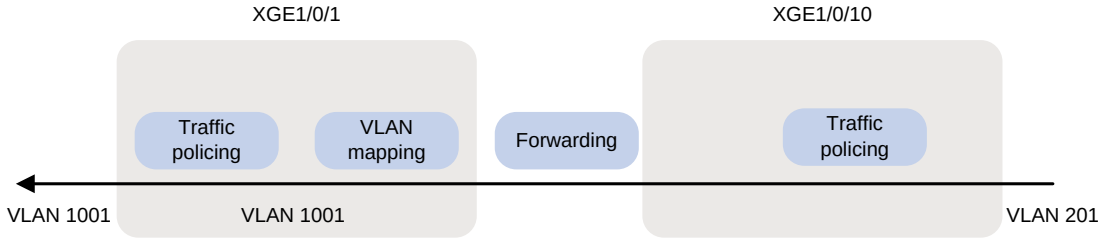


Figure 4 shows how the switches process the downlink traffic from the backbone network to a branch. The figure uses VLAN 201 as an example.

Figure 4 Downlink traffic processing



Verifying the configuration

Verify the configuration on any interface, for example, GigabitEthernet 1/0/10.

Verify QoS policies applied to interface GigabitEthernet 1/0/10.

```
[Device] display qos policy interface gigabitethernet 1/0/10
Interface: GigabitEthernet1/0/10
  Direction: Inbound
  Policy: BONEupdown
   Classifier: vlan201
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 201
     Behavior: car100
      Committed Access Rate:
        CIR 102400 (kbps), CBS 6400000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: vlan202
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 202
     Behavior: car60
      Committed Access Rate:
        CIR 61440 (kbps), CBS 3840000 (Bytes), EBS 0 (Bytes)
```

```
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: vlan203
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 203
     Behavior: car40
      Committed Access Rate:
        CIR 40960 (kbps), CBS 2560000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
Interface: GigabitEthernet1/0/10
  Direction: Outbound
  Policy: BONEupdown
   Classifier: vlan201
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 201
     Behavior: car100
      Committed Access Rate:
        CIR 102400 (kbps), CBS 6400000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: vlan202
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 202
     Behavior: car60
      Committed Access Rate:
        CIR 61440 (kbps), CBS 3840000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: vlan203
     Operator: AND
     Rule(s) :
      If-match customer-vlan-id 203
```

```
     Behavior: car40
      Committed Access Rate:
        CIR 40960 (kbps), CBS 2560000 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Configuration files

```
#
traffic classifier vlan201 operator and
 if-match customer-vlan-id 201
#
traffic classifier vlan202 operator and
 if-match customer-vlan-id 202
#
traffic classifier vlan203 operator and
 if-match customer-vlan-id 203
#
traffic behavior car40
 car cir 40960 cbs 2560000 ebs 0 green pass red discard yellow pass
#
traffic behavior car60
 car cir 61440 cbs 3840000 ebs 0 green pass red discard yellow pass
#
traffic behavior car100
 car cir 102400 cbs 6400000 ebs 0 green pass red discard yellow pass
#
traffic behavior car200
 car cir 204800 cbs 12800000 ebs 0 green pass red discard yellow pass
#
traffic behavior car400
 car cir 409600 cbs 25600000 ebs 0 green pass red discard yellow pass
#
qos policy ABCupdown
 classifier vlan201 behavior car400
 classifier vlan202 behavior car200
 classifier vlan203 behavior car200
#
qos policy BONEupdown
 classifier vlan201 behavior car100
 classifier vlan202 behavior car60
 classifier vlan203 behavior car40
#
interface GigabitEthernet1/0/10
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203
 qos apply policy BONEupdown inbound
 qos apply policy BONEupdown outbound
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003
 vlan mapping 1001 translated-vlan 201
 vlan mapping 1002 translated-vlan 202
 vlan mapping 1003 translated-vlan 203
 qos apply policy ABCupdown inbound
 qos apply policy ABCupdown outbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203 1001 to 1003
 vlan mapping 1001 translated-vlan 201
 vlan mapping 1002 translated-vlan 202
 vlan mapping 1003 translated-vlan 203
 qos apply policy ABCupdown inbound
 qos apply policy ABCupdown outbound
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 201 to 203
 qos apply policy ABCupdown inbound
 qos apply policy ABCupdown outbound
#
```

Example: Configuring aggregate CAR

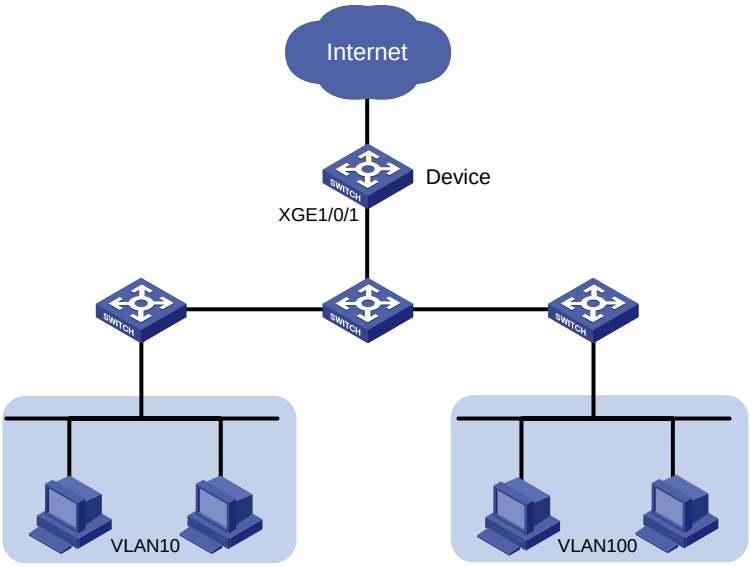
Network configuration

As shown in Figure 5, the access layer devices add VLAN tags to the traffic from VLAN 10 and VLAN 100 before sending the traffic to the device.

Configure aggregate CAR on GigabitEthernet 1/0/1 to meet the following requirements:

- Limit the incoming traffic from VLAN 10 and VLAN 100 to 200 Mbps.
- Drop the excess traffic.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series	Release 63xx

MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Procedures

Configure interface GigabitEthernet 1/0/1 as a trunk port.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
```

Assign the interface to VLANs 10 and 100.

```
[Device-GigabitEthernet1/0/1] port trunk permit vlan 10 100
```

Remove the interface from VLAN 1.

```
[Device-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Device-GigabitEthernet1/0/1] quit
```

Create an aggregate CAR action.

```
[Device] qos car aggcar-1 aggregative cir 204800
```

Create class 1, and use SVLAN ID 10 as the match criterion.

```
[Device] traffic classifier 1
[Device-classifier-1] if-match service-vlan-id 10
[Device-classifier-1] quit
```

Create behavior 1, and reference the aggregate CAR action in the behavior.

```
[Device] traffic behavior 1
[Device-behavior-1] car name aggcar-1
[Device-behavior-1] quit
```

Create class 2, and use SVLAN ID 100 as the match criterion.

```
[Device] traffic classifier 2
[Device-classifier-2] if-match service-vlan-id 100
[Device-classifier-2] quit
```

Create behavior 2, and reference the aggregate CAR action in the behavior.

```
[Device] traffic behavior 2
[Device-behavior-2] car name aggcar-1
[Device-behavior-2] quit
```

Create a QoS policy named **car**, and associate the classes with the behaviors in the QoS policy.

```
[Device] qos policy car
[Device-qospolicy-car] classifier 1 behavior 1
[Device-qospolicy-car] classifier 2 behavior 2
[Device-qospolicy-car] quit
```

Apply the QoS policy **car** to the inbound direction of GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy car inbound
```

Verifying the configuration

Verify the configuration on any interface, for example, GigabitEthernet 1/0/1.

Verify QoS policies applied to interface GigabitEthernet 1/0/1.

```
[Device] display qos policy interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: car
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match service-vlan-id 10
     Behavior: 1
      Committed Access Rate:
        Car name: aggcar-1
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match service-vlan-id 100
     Behavior: 2
      Committed Access Rate:
        Car name: aggcar-1
```

Configuration files

```
#
```

```
 qos car aggcar-1 aggregative cir 204800 cbs 12800000 ebs 0 green pass yellow pass
red discard
#
traffic classifier 1 operator and
 if-match service-vlan-id 10
traffic classifier 2 operator and
 if-match service-vlan-id 100
#
traffic behavior 1
 car name aggcar-1
traffic behavior 2
 car name aggcar-1
#
qos policy car
 classifier 1 behavior 1
 classifier 2 behavior 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 100
 qos apply policy car inbound
```

Contents

Introduction

This document provides GTS and rate limiting configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of GTS and rate limiting.

Example: Configuring GTS and rate limiting

Network configuration

As shown in Figure 1, the 15-Mbps dedicated line transmits the FTP traffic, business-specific application traffic, and IP voice traffic between the headquarters and branch of a company.

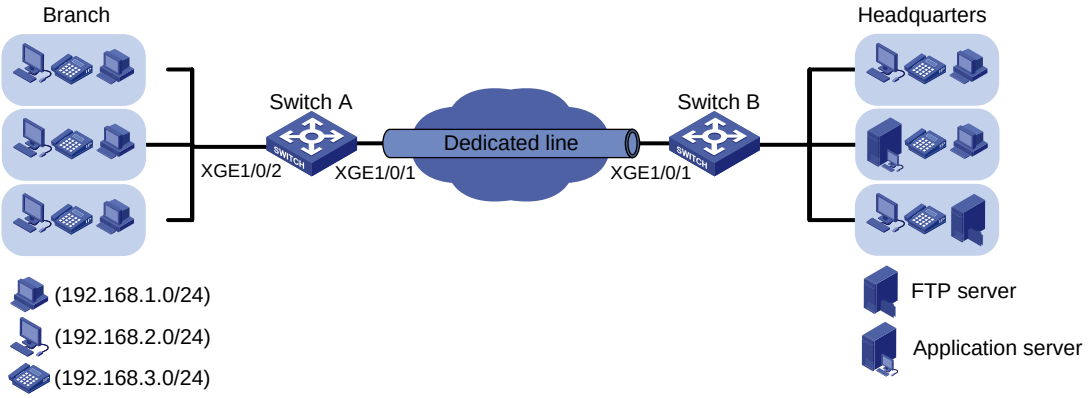
The following traffic policing settings have been configured on the edge device (Switch B) of the headquarters:

- CIR of 10 Mbps for IP voice traffic.
- CIR of 3 Mbps for business-specific application traffic.
- CIR of 7 Mbps for FTP traffic.

Configure traffic shaping on the edge device (Switch A) of the branch to buffer excess traffic of each traffic type.

Configure rate limiting on Switch A to limit the outgoing traffic rate to 15 Mbps.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To implement GTS, first determine the queue that transmits a type of traffic. In this example, the priorities of these types of traffic are not provided. You need to use priority marking to manually assign packets to different queues.
- You can manually assign packets to queues by marking DSCP values, 802.1p priority values, or local precedence values. To keep the contents of packets unchanged, mark local precedence values for packets.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series	Release 63xx

IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Procedures

Before configuring GTS and rate limiting, make sure there is network connectivity between the branch and headquarters.

This section does not describe the configurations for enabling network connectivity.

Configuring priority marking

1. Create three traffic classes to match the three traffic types:

Configure basic IPv4 ACL 2000 to match IP voice traffic (traffic from subnet 192.168.3.0/24).

```
<SwitchA> system-view
[SwitchA] acl basic 2000
[SwitchA-acl-ipv4-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[SwitchA-acl-ipv4-basic-2000] quit
```

Create a class named **voice**, and use ACL 2000 as the match criterion.

```
[SwitchA] traffic classifier voice
[SwitchA-classifier-voice] if-match acl 2000
[SwitchA-classifier-voice] quit
```

Configure basic IPv4 ACL 2001 to match application traffic (traffic from subnet 192.168.2.0/24).

```
[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[SwitchA-acl-ipv4-basic-2001] quit
```

Create a class named **service**, and use ACL 2001 as the match criterion.

```
[SwitchA] traffic classifier service
[SwitchA-classifier-service] if-match acl 2001
[SwitchA-classifier-service] quit
```

Configure advanced IPv4 ACL 3000 to match FTP traffic (traffic from subnet 192.168.1.0/24 and with destination port number 20).

```
[SwitchA] acl advanced 3000
[SwitchA-acl-ipv4-adv-3000] rule permit tcp destination-port eq 20 source
192.168.1.0 0.0.0.255
[SwitchA-acl-ipv4-adv-3000] quit
```

Create a class named **ftp**, and use ACL 3000 as the match criterion.

```
[SwitchA] traffic classifier ftp
[SwitchA-classifier-ftp] if-match acl 3000
[SwitchA-classifier-ftp] quit
```

2. Create three traffic behaviors:

Create a behavior named **voice**, and configure the behavior to mark packets with local precedence 6 (corresponding to queue 6).

```
[SwitchA] traffic behavior voice
[SwitchA-behavior-voice] remark local-precedence 6
[SwitchA-behavior-voice] quit
```

Create a behavior named **service**, and configure the behavior to mark packets with local precedence 4 (corresponding to queue 4).

```
[SwitchA] traffic behavior service
[SwitchA-behavior-service] remark local-precedence 4
[SwitchA-behavior-service] quit
```

Create a behavior named **ftp**, and configure the behavior to mark packets with local precedence 2 (corresponding to queue 2).

```
[SwitchA] traffic behavior ftp
[SwitchA-behavior-ftp] remark local-precedence 2
[SwitchA-behavior-ftp] quit
```

3. Configure and apply a QoS policy:

Create a QoS policy named **shaping**, and associate the three classes with their respective behaviors in the QoS policy.

```
[SwitchA] qos policy shaping
[SwitchA-qospolicy-shaping] classifier voice behavior voice
[SwitchA-qospolicy-shaping] classifier service behavior service
[SwitchA-qospolicy-shaping] classifier ftp behavior ftp
[SwitchA-qospolicy-shaping] quit
```

Apply the QoS policy **shaping** to the inbound direction of GigabitEthernet 1/0/2.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos apply policy shaping inbound
[SwitchA-GigabitEthernet1/0/2] quit
```

Configuring GTS

Configure GTS on GigabitEthernet 1/0/1 to set the CIR to 10 Mbps for queue 6 (IP voice traffic).

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos gts queue 6 cir 10240
```

Configure GTS on GigabitEthernet 1/0/1 to set the CIR to 3 Mbps for queue 4 (application traffic).

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 4 cir 3072
```

Configure GTS on GigabitEthernet 1/0/1 to set the CIR to 7 Mbps for queue 2 (FTP traffic).

```
[SwitchA-GigabitEthernet1/0/1] qos gts queue 2 cir 7168
```

Configuring rate limiting

Configure rate limiting on GigabitEthernet 1/0/1 to set the CIR to 15 Mbps for outgoing traffic.

```
[SwitchA-GigabitEthernet1/0/1] qos lr outbound cir 15360
```

Verifying the configuration

Verify the priority marking settings of GigabitEthernet 1/0/2.

```
<Sysname> display qos policy interface inbound
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: shaping
   Classifier: voice
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: voice
      Marking:
        Remark local-precedence 6
   Classifier: service
     Operator: AND
     Rule(s) :
      If-match acl 2001
     Behavior: service
      Marking:
        Remark local-precedence 4
   Classifier: ftp
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: ftp
      Marking:
        Remark local-precedence 2
```

Verify the GTS settings on GigabitEthernet 1/0/1.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule: If-match queue 6
  CIR 10240 (kbps), CBS 640000 (Bytes)
 Rule: If-match queue 4
  CIR 3072 (kbps), CBS 192000 (Bytes)
 Rule: If-match queue 2
  CIR 7168 (kbps), CBS 448000 (Bytes)
```

Verify the rate limiting settings on GigabitEthernet 1/0/1.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 15360 (kbps), CBS 960000 (Bytes)
```

Configuration files

```
#
acl basic 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
#
acl basic 2001
 rule 0 permit source 192.168.2.0 0.0.0.255
#
acl advanced 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp-data
#
traffic classifier ftp operator and
 if-match acl 3000
#
traffic classifier service operator and
 if-match acl 2001
#
traffic classifier voice operator and
 if-match acl 2000
#
traffic behavior ftp
 remark local-precedence 2
#
traffic behavior service
 remark local-precedence 4
#
traffic behavior voice
 remark local-precedence 6
#
qos policy shaping
 classifier voice behavior voice
 classifier service behavior service
 classifier ftp behavior ftp
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos lr outbound cir 15360 cbs 960000
 qos gts queue 6 cir 10240 cbs 640000
 qos gts queue 4 cir 3072 cbs 192000
 qos gts queue 2 cir 7168 cbs 448000
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos apply policy shaping inbound
#
return
```

Contents

Introduction

This document provides traffic filtering configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of traffic filtering.

Example: Configuring traffic filtering

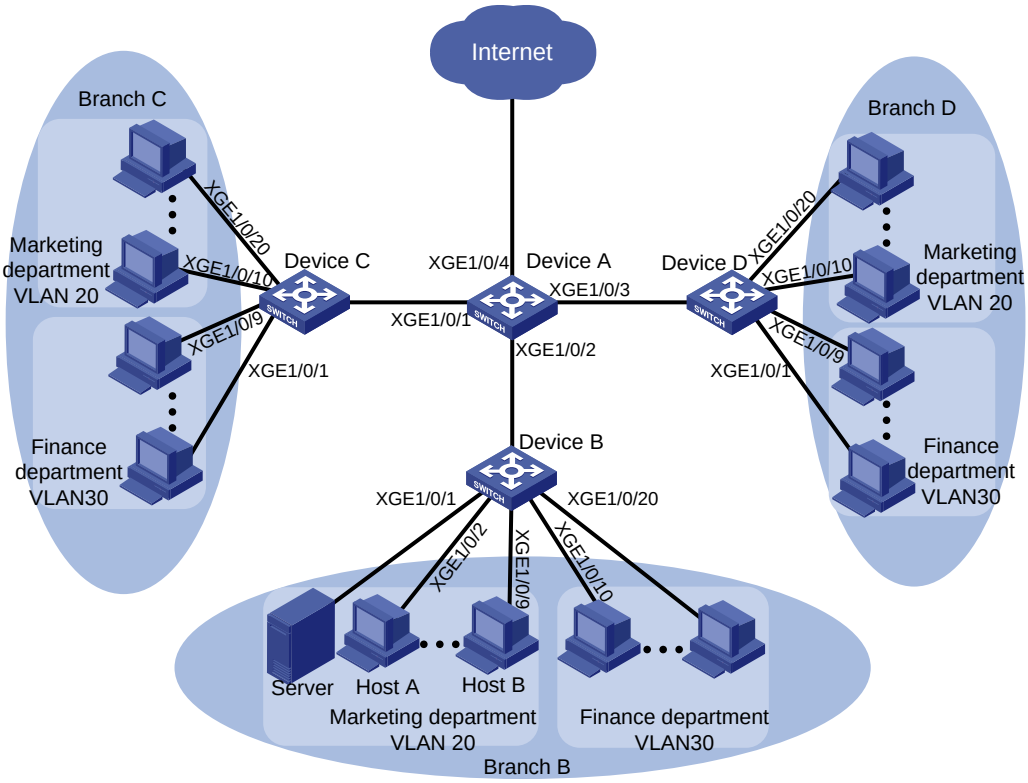
Network configuration

As shown in Figure 1, a company has three branches, each of which has a Marketing department and a Finance department. All Marketing departments belong to VLAN 20. All Finance departments belong to VLAN 30.

Configure traffic filtering to meet the following requirements:

- HTTP traffic from the Marketing department in each branch is denied.
- In Branch B, only Host A and Host B can access the server.
- The Marketing departments in three branches can access one another, and the Finance departments in three branches can access one another.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To deny HTTP traffic from the Marketing departments, use one of the following methods:
  - Filter outgoing traffic from the subnet 192.168.4.0/24 on the interfaces that connect Device B, Device C, and Device D to Device A.

    This method has poor scalability, because new branches require the same configuration on their access switches.
  - Filter outgoing traffic from the subnet 192.168.4.0/24 on interface GigabitEthernet 1/0/4 of Device A.

    This method wastes processing capabilities of Device A, because Device A must internally forward all incoming traffic to interface GigabitEthernet 1/0/4.
  - Configure a QoS policy to deny HTTP traffic from the Marketing departments.

    This method can automatically adapt to changing network topologies and also saves hardware resources by denying traffic on the incoming interface. This example uses this method.
- To allow only Host A and Host B to access the server in Branch B, perform the following tasks:
  - Configure an ACL on GigabitEthernet 1/0/1 to allow packets from 192.168.4.10/24 and 192.168.4.15/24.

    - Set the default packet filtering action to **deny** to deny packets that do not match the configured ACL.
- To allow traffic from Marketing departments and Finance departments (except HTTP traffic) to the Internet and to allow access among Marketing departments and among Finance departments, perform the following tasks:
    - Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 as trunk ports.
    - Assign these interfaces to VLAN 20 and VLAN 30.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- S5130S-HI series.
- S5130S-EI series.
- S3100V3-EI series.
- E128C switch.
- E152C switch.
- E500C series.
- E500D series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M series.
- IE4320 series.

Restrictions and guidelines

If a traffic behavior is configured with the **filter deny** action, all other actions in the same QoS policy except traffic accounting do not take effect.

Procedures

Configuring Device A

Create VLAN 20 and VLAN 30.

```
<DeviceA> system-view
[DeviceA] vlan 20
[DeviceA-vlan20] quit
[DeviceA] vlan 30
[DeviceA-vlan30] quit
```

Add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to interface range named **myport**.

```
[DeviceA] interface range name myport interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/4
```

Configures interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 as trunk ports, assign them to VLAN 20 and VLAN 30, and remove them from VLAN 1.

```
[DeviceA-if-range-myport] port link-type trunk
[DeviceA-if-range-myport] port trunk permit vlan 20 30
[DeviceA-if-range-myport] undo port trunk permit vlan 1
[DeviceA-if-range-myport] quit
```

Configure advanced IPv4 ACL 3000 to match HTTP traffic from subnet 192.168.4.0/24.

```
[DeviceA] acl advanced 3000
```

```
[DeviceA-acl-ipv4-adv-3000] rule deny tcp source 192.168.4.0 0.0.0.255 source-port eq
80
[DeviceA-acl-ipv4-adv-3000] quit
```

Create a class named **vlan20_http**, and use ACL 3000 as the match criterion.

```
[DeviceA] traffic classifier vlan20_http
[DeviceA-classifier-vlan20_http] if-match acl 3000
[DeviceA-classifier-vlan20_http] quit
```

Create a behavior named **vlan20_http**, and configure traffic filtering to deny traffic of the class **vlan20_http**.

```
[DeviceA] traffic behavior vlan20_http
[DeviceA-behavior-vlan20_http] filter deny
[DeviceA-behavior-vlan20_http] quit
```

Create a QoS policy named **vlan20_http**, and associate the class **vlan20_http** with the behavior **vlan20_http** in the QoS policy.

```
[DeviceA] qos policy vlan20_http
[DeviceA-qospolicy-vlan20_http] classifier vlan20_http behavior vlan20_http
[DeviceA-qospolicy-vlan20_http] quit
```

Apply the QoS policy **vlan20_http** to the inbound direction of VLAN 20 and VLAN 30.

```
[DeviceA] qos vlan-policy vlan20_http vlan 20 30 inbound
```

Configuring Device B

Configure basic IPv4 ACL 2000 to permit traffic from Host A and Host B.

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 192.168.4.10 0
[DeviceB-acl-ipv4-basic-2000] rule permit source 192.168.4.15 0
[DeviceB-acl-ipv4-basic-2000] quit
```

Set the packet filtering default action to **deny**.

```
[DeviceB] packet-filter default deny
```

Apply ACL 2000 to interface GigabitEthernet 1/0/1 to filter outgoing traffic.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] packet-filter 2000 outbound
```

Verifying the configuration

Verify the QoS policy applied to the inbound direction of VLAN 20 and VLAN 30.

```
[DeviceA]display qos vlan-policy vlan inbound
  Direction: Inbound
  Policy: vlan20_http
   Classifier: vlan20_http
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: vlan20_http
      Filter enable: Deny
Vlan 30
  Direction: Inbound
```

```
  Policy: vlan20_http
   Classifier: vlan20_http
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: vlan20_http
      Filter enable: Deny
```

Display application details of ACLs for incoming packet filtering on GigabitEthernet 1/0/1.

```
[DeviceB] display packet-filter verbose interface gigabitethernet 1/0/1 outbound
Interface: GigabitEthernet1/0/1
 Outbound policy:
  IPv4 ACL 2000
   rule 0 permit source 192.168.4.10 0
  IPv4 default action: Deny
```

Configuration files

- Device A:

```
#
vlan 20
#
vlan 30
#
interface range name myport interface GigabitEthernet1/0/1 to
GigabitEthernet1/0/4
#
acl advanced 3000
 rule 0 deny tcp source 192.168.4.0 0.0.0.255 source-port eq www
#
traffic classifier vlan20_http operator and
 if-match acl 3000
#
traffic behavior vlan20_http
 filter deny
#
qos policy vlan20_http
 classifier vlan20_http behavior vlan20_http
#
 qos vlan-policy vlan20_http vlan 20 inbound
 qos vlan-policy vlan20_http vlan 30 inbound
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20 30
```

- Device B:

```
#
acl basic 2000
 rule 0 permit source 192.168.4.10 0
#
 packet-filter default deny
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 packet-filter 2000 outbound
#
```

Contents

Introduction

This document provides AAA configuration examples for Telnet and SSH users.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of AAA.

Example: Configuring HWTACACS authentication and authorization in ACS for Telnet users

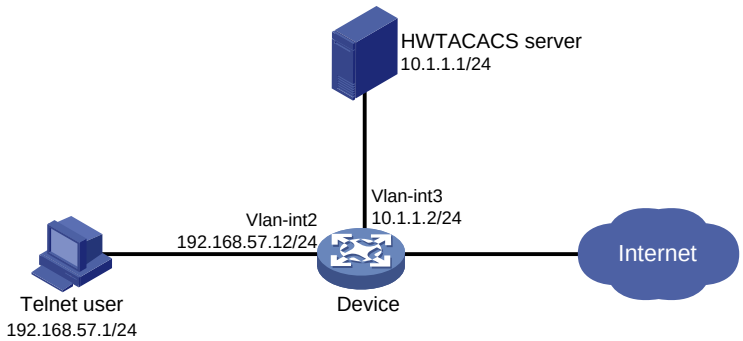
Network configuration

As shown in Figure 1, configure the device to meet the following requirements:

- The HWTACACS server is used to provide authentication and authorization services for Telnet users.
- The authenticated users are permitted to execute the **`display`** commands of all system features and resources.

Add a user account with username **user@bbb** and password **123456TESTplat&!** on the HWTACACS server.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the Telnet username and password on the HWTACACS server to identify valid users.
- For Telnet users to perform AAA, set the authentication mode to **scheme** on VTY user lines.

- Configure the same shared key on the device and the HWTACACS server to secure HWTACACS communication. When the shared key is configured, the device and the HWTACACS server transfer passwords safely and the device can verify the integrity of each HWTACACS response.
- Configure HWTACACS authentication and authorization by performing the following tasks on the device:
  - Create an HWTACACS scheme.
  - Specify the authentication and authorization servers.
  - Apply the HWTACACS scheme to the ISP domain to which the Telnet users belong on the device.
- Configure the HWTACACS server to assign the **network-operator** user role to the users, so the users can use all **`display`** commands.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx

Hardware	Software version
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI	Release 6810 and later versions

Procedures

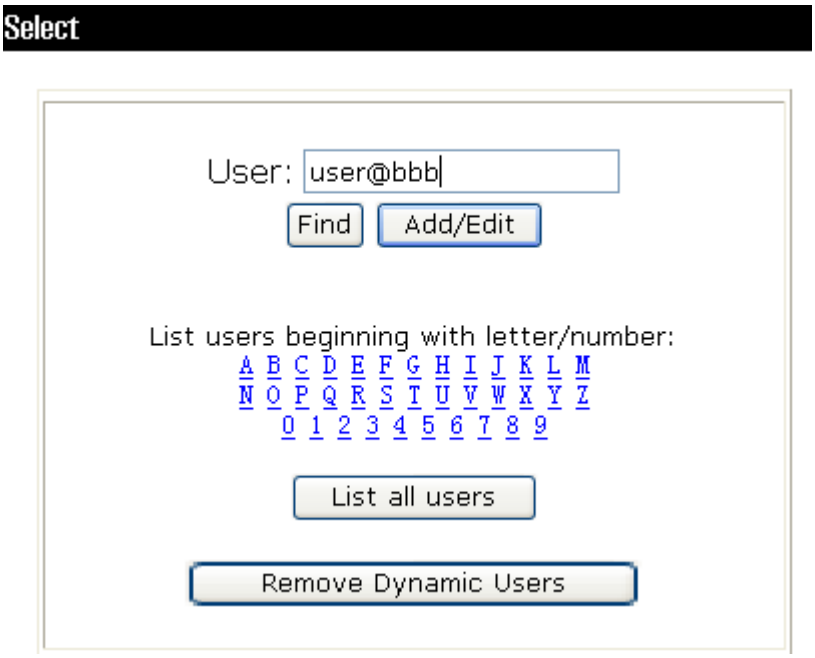
Configuring the HWTACACS server

In this example, the server runs ACS 4.0.

Adding a user

1. In the navigation tree, click **User Setup**.
2. Enter **user@bbb** in the **User** field and click **Add/Edit**, as shown in Figure 2.

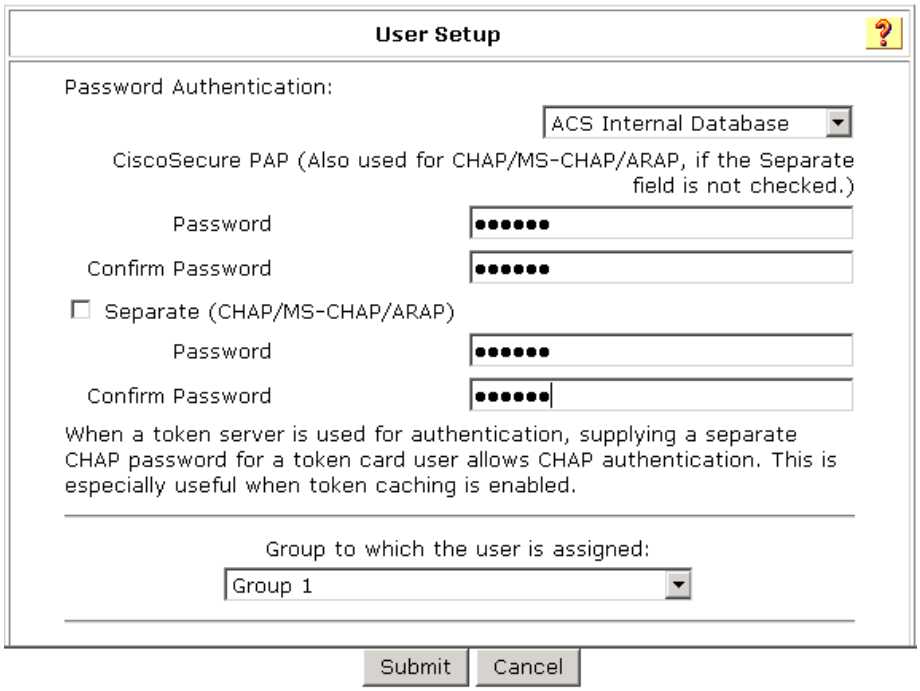
Figure 2 Adding a user



Configuring the user

1. On the **User Setup** page, configure the following parameters, as shown in Figure 3:
   - Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.
   - Assign the user to user group **Group 1**.

Figure 3 Configuring the user password



2. Click **Submit**.

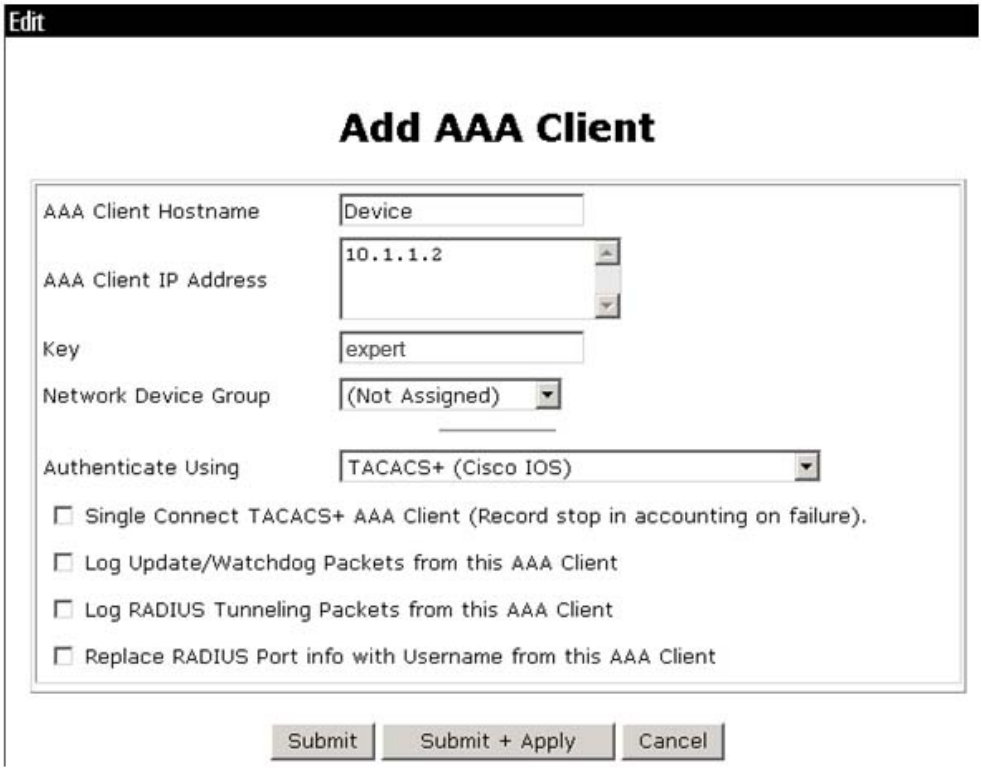
Configuring the network settings

1. In the navigation tree, click **Network Configuration**.
2. On the **Add AAA Client** page, configure the following parameters, as shown in Figure 4:
   - Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
   - Enter **10.1.1.2** in the **AAA Client IP Address** field.

     The IP address is the source IP address for outgoing HWTACACS packets on the device.
   - Enter **expert** in the **Key** field.

     The key configured here is the same as the authentication, authorization, and accounting keys configured on the device for secure HWTACACS communication.
   - Select **TACACS+ (Cisco IOS)** from the **Authenticate Using** list.

Figure 4 Configuring the network settings

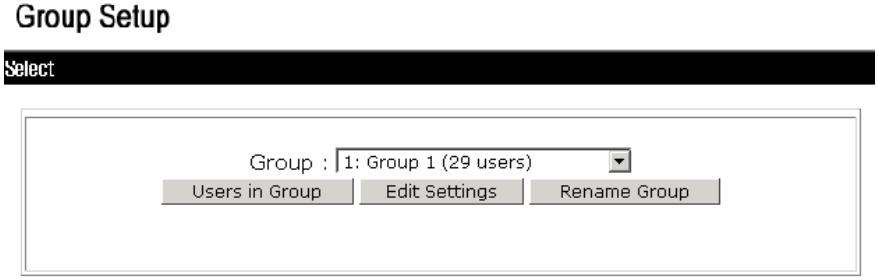


3. Click **Submit + Apply**.

Configuring the user group

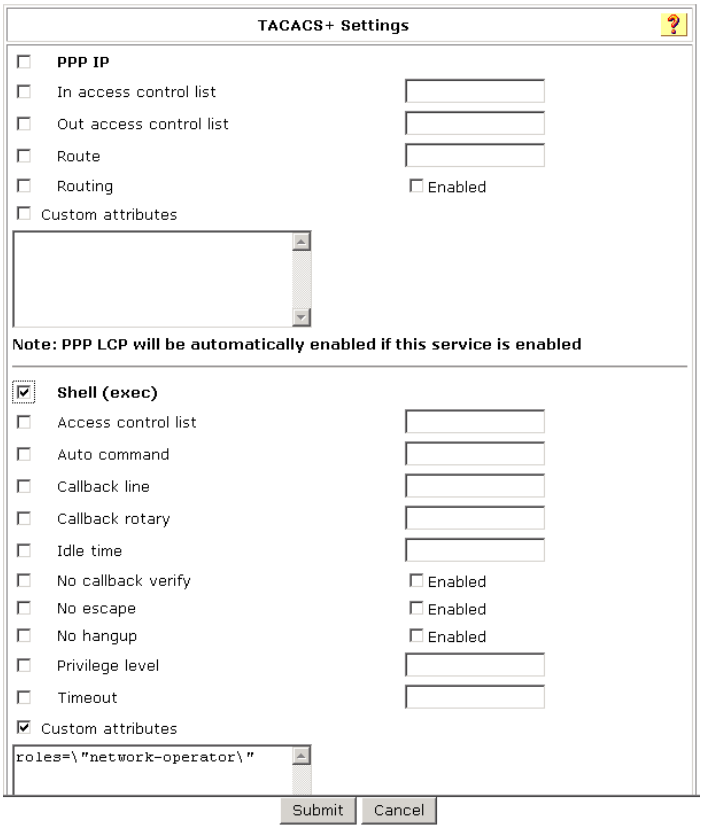
1. In the navigation tree, click **Group Setup**.
2. Select **1: Group 1 (29 users)** from the **Group** list and click **Edit Settings**, as shown in Figure 5.

Figure 5 Selecting a user group



3. On the **TACACS+ Settings** page, configure the following parameters, as shown in Figure 6:
   - Select **Shell(exec)**, which enables command execution for all users in the group.
   - Select **Custom attributes**, and enter **roles=\"network-operator\"** in the **Custom attributes** field.
   - Configure other settings as needed.

Figure 6 Configuring the user group



4. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.57.12 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Enable the Telnet server feature.

```
[Device] telnet server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create an HWTACACS scheme named **hwtac**.

```
[Device] hwtacacs scheme hwtac
```

Specify the primary HWTACACS server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS server.

```
[Device-hwtacacs-hwtac] key authentication simple expert
[Device-hwtacacs-hwtac] key authorization simple expert
[Device-hwtacacs-hwtac] key accounting simple expert
[Device-hwtacacs-hwtac] quit
```

Create an ISP domain named **bbb**, and specify the domain to use HWTACACS scheme **hwtac** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit
```

Verifying the configuration

Telnet to the device, and enter username **user@bbb** and password **123456TESTplat&!**. The user logs into the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.57.12 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
hwtacacs scheme hwtac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$X3oR/wjLFjDqIyjdAmvjwAhiuqewGABglQ==
 key authorization cipher $c$3$5pmuq0RJ9UWMWDkRNNERX6HFM0aRv5txFg==
 key accounting cipher $c$3$FSdSiBY1u+ZNkAYYlPw9YkGxJA4iR8MDjw==
#
 domain bbb
  authentication login hwtacacs-scheme hwtac
  authorization login hwtacacs-scheme hwtac
  accounting login hwtacacs-scheme hwtac
#
```

Example: Configuring RADIUS authentication and authorization in IMC for SSH users

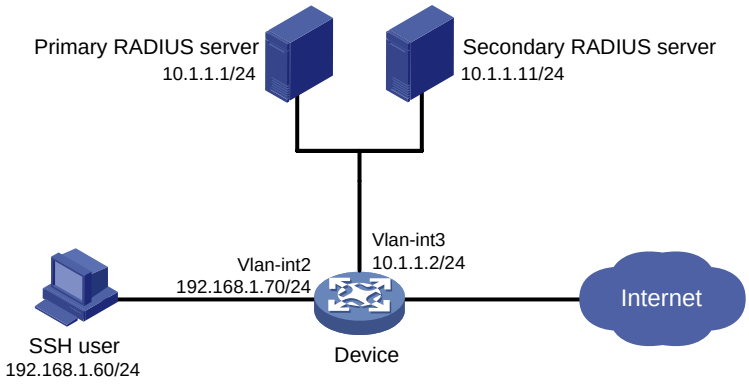
Network configuration

As shown in Figure 7, configure the device to meet the following requirements:

- The RADIUS servers are used to provide authentication and authorization services for SSH users. One server acts as the primary server and the other acts as the secondary server.
- Domain names are included in the usernames sent to the RADIUS servers.
- The authenticated users are permitted to use the **`display`** commands of all system features and resources.

The RADIUS servers run IMC. Add a user account with username **hello@bbb** and password **123456TESTplat&!** on each RADIUS server.

Figure 7 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the primary and secondary RADIUS servers to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY user lines.
- Configure the same shared key on the device and the RADIUS servers to secure RADIUS communication. When the shared key is configured, the device and the RADIUS servers transfer passwords safely and the device can verify the integrity of each RADIUS response.
- Configure RADIUS authentication and authorization by performing the following tasks on the device:
  - Create a RADIUS scheme.
  - Specify the primary and secondary servers for authentication and authorization.
  - Apply the RADIUS scheme to the ISP domain to which the SSH users belong.
- Configure the RADIUS servers to assign the **network-operator** user role to the users, so the users can use all **`display`** commands.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx

Hardware	Software version
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx

Hardware	Software version
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI	Release 6810 and later versions

Restrictions and guidelines

When you configure RADIUS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring RADIUS servers

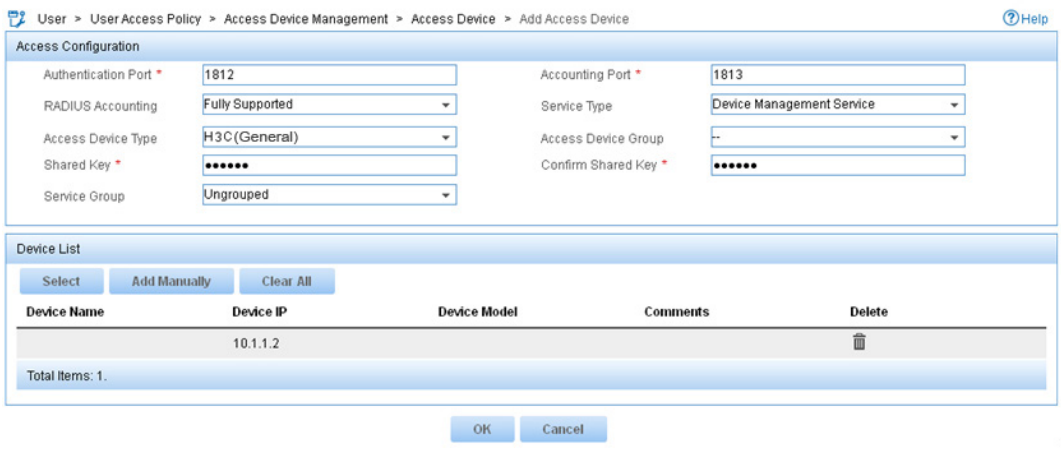
In this example, RADIUS servers run IMC PLAT 7.0 (E0102) and IMC UAM 7.0 (E0201). This example describes the configuration of the primary RADIUS server. Configure the secondary RADIUS server in the same way the primary RADIUS server is configured.

Adding the device to IMC as an access device

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.

   The access device list appears.
3. Click **Add**.
4. On the **Add Access Device** page, configure the following parameters, as shown in Figure 8:
   - Enter **1812** and **1813** in the **Authentication Port** and **Accounting Port** fields, respectively.
   - Enter **expert** in the **Shared Key** and **Confirm Shared Key** fields.
   - Select **Device Management Service** from the **Service Type** list.
   - Select **H3C(General)** from the **Access Device Type** list.
   - Use the default values for other parameters in the **Access Configuration** area.
   - In the **Device List** area, click **Select** or **Add Manually** to add the device (10.1.1.2) to IMC as an access device.

   Figure 8 Adding an access device



5. Click **OK**.

Adding a device management user

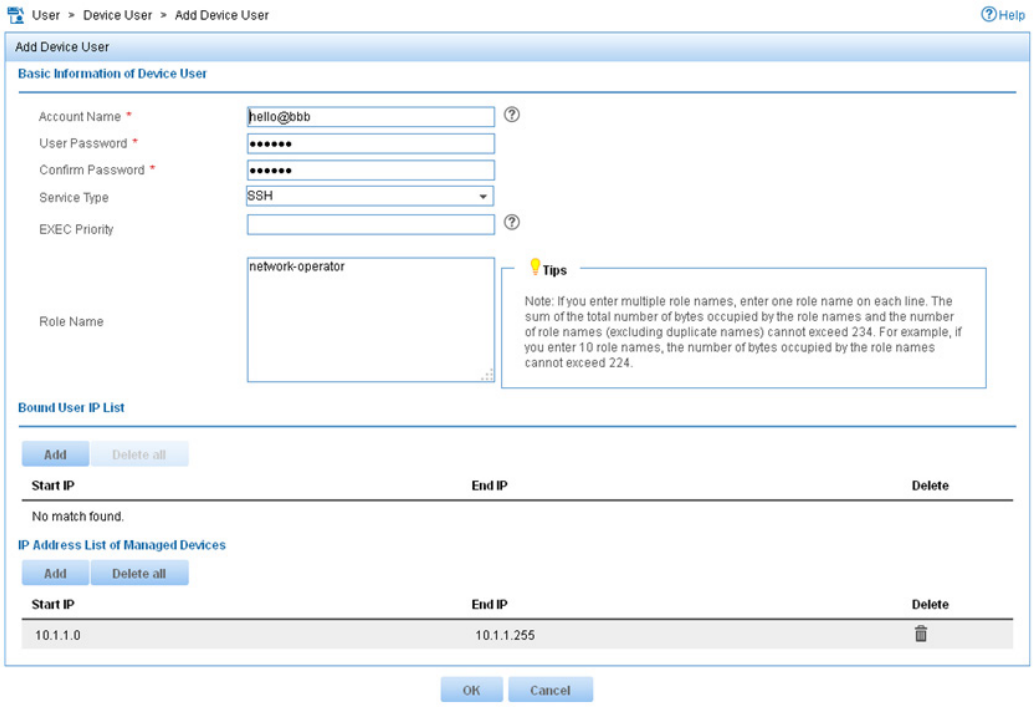
1. Click the **User** tab.
2. From the navigation tree, select **Access User** > **Device User**.

   The device management user list appears.
3. Click **Add**.
4. On the **Add Device User** page, configure the following parameters, as shown in Figure 9:
   - Enter **hello@bbb** in the **Account Name** field.
   - Enter **aabbcc** in the **User Password** and **Confirm Password** fields.

- Select **SSH** from the **Service Type** list.
- Enter **network-operator** in the **Role Name** field.

  The network-operator user role has access to the **display** commands of all system features and resources.
- In the **IP Address List of Managed Devices** area, click **Add** to specify an IP segment (from 10.1.1.0 to 10.1.1.255) for management. The IP segment must contain the IP address of the access device.

Figure 9 Adding a device management user



5. Click **OK**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
```

```
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..........
Create the key pair successfully.
```

Create a local DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.......
Create the key pair successfully.
```

Create a 256-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

Create a 384-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create a RADIUS scheme named **rad**.

```
[Device] radius scheme rad
```

Specify the primary authentication RADIUS server with the IP address 10.1.1.1 and port number 1812.

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the secondary authentication RADIUS server with the IP address 10.1.1.11 and port number 1812.

```
[Device-radius-rad] secondary authentication 10.1.1.11 1812
```

Specify the primary accounting RADIUS server with the IP address 10.1.1.1 and port number 1813.

```
[Device-radius-rad] primary accounting 10.1.1.1 1813
```

Specify the secondary accounting RADIUS server with the IP address 10.1.1.11 and port number 1813.

```
[Device-radius-rad] secondary accounting 10.1.1.11 1813
```

Set the authentication and accounting shared keys to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-rad] key authentication simple expert
[Device-radius-rad] key accounting simple expert
```

Include domain names in the usernames sent to the RADIUS server.

```
[Device-radius-rad] user-name-format with-domain
[Device-radius-rad] quit
```

Create an ISP domain named **bbb**, and configure the ISP domain to use the RADIUS scheme **rad** as the AAA methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login radius-scheme rad
[Device-isp-bbb] quit
```

Verifying the configuration

Initiate an SSH connection to the device, and enter username **hello@bbb** and password **123456TESTplat&!**. The user logs into the device. (Details not shown.)

Verify that the user can use the **display** commands of all system features and resources. (Details not shown.)

(Release 6008 and later on the S6550XE-HI switch series and S6525XE-HI switch series, and Release 8005 and later on the S5850 switch series.) Display RADIUS scheme configuration.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes


------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    Host name: Not Configured
    IP   : 10.1.1.1                                Port: 1812
    VPN  : Not configured
    State: Active (duration: 0 weeks, 0 days, 0 hours, 2 minutes, 2 seconds)
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
    Host name: Not Configured
    IP   : 10.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 37 seconds)
    Weight: 0
  Second authentication server:
    Host name: Not Configured
    IP   : 10.1.1.11                               Port: 1812
```

```
    VPN  : Not configured
    State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 50 seconds)
    Test profile: Not configured
    Weight: 0
  Second accounting server:
    Host name: Not Configured
    IP   : 10.1.1.11                              Port: 1813
    VPN  : Not configured
    State: Active (duration: 0 weeks, 0 days, 0 hours, 1 minutes, 23 seconds)
    Weight: 0
  Accounting-On function                    : Disabled
    extended function                       : Disabled
    retransmission times                    : 50
    retransmission interval(seconds)        : 3
  Timeout Interval(seconds)                 : 3
  Retransmission Times                      : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)              : 5
  Realtime Accounting Interval(seconds)     : 720
  Stop-accounting packets buffering         : Enabled
    Retransmission times                    : 500
  NAS IP Address                            : Not configured
  VPN                                       : Not configured
  User Name Format                          : with-domain
  Data flow unit                            : Byte
  Packet unit                               : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                              : Standard
  Attribute Remanent-Volume unit            : Kilo
  server-load-sharing                       : Disabled
  Attribute 31 MAC format                   : HH-HH-HH-HH-HH-HH
  Stop-accounting packets send-force        : Disabled
  Reauthentication server selection         : Inherit
  Attribute 218 of vendor ID 25506          : DHCP-Option 61
                                              Format 1 (1-byte Type field)
```

(Release 63xx.) Display RADIUS scheme configuration.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

-------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    Host name: Not Configured
    IP   : 10.1.1.1                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
```

```
    Weight: 0
  Primary accounting server:
    Host name: Not Configured
    IP   : 10.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Second authentication server:
    Host name: Not Configured
    IP   : 10.1.1.11                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Second accounting server:
    Host name: Not Configured
    IP   : 10.1.1.11                               Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Accounting-On function                     : Disabled
    extended function                        : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 720
  Stop-accounting packets buffering          : Enabled
    Retransmission times                     : 500
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : Standard
  Attribute Remanent-Volume unit             : Kilo
  server-load-sharing                        : Disabled
  Attribute 31 MAC format                    : HH-HH-HH-HH-HH-HH
  Stop-accounting packets send-force         : Disabled
  Reauthentication server selection          : Inherit
```

(R65xx.) Display RADIUS scheme configuration.

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

------------------------------------------------------------------
```

```
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    Host name: Not Configured
    IP   : 10.1.1.1                                Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
    Host name: Not Configured
    IP   : 10.1.1.1                                Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Second authentication server:
    Host name: Not Configured
    IP   : 10.1.1.11                               Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Second accounting server:
    Host name: Not Configured
    IP   : 10.1.1.11                               Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Accounting-On function                     : Disabled
    extended function                        : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 720
  Stop-accounting packets buffering          : Enabled
    Retransmission times                     : 500
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : Standard
  Attribute Remanent-Volume unit             : Kilo
  server-load-sharing                        : Disabled
```

```
  Attribute 30 format                        : HH-HH-HH-HH-HH-HH:SSID
  Attribute 30 MAC format                    : HH-HH-HH-HH-HH-HH
  Attribute 31 MAC format                    : HH-HH-HH-HH-HH-HH
  Stop-accounting packets send-force         : Disabled
  Reauthentication server selection          : Inherit
  Attribute 218 of vendor ID 25506           : DHCP-Option 61
                                               Format 1 (1-byte Type field)
```

The output shows that the primary RADIUS server is in **Active** state.

Disconnect the device from the primary RADIUS server. (Details not shown.)

Verify that the primary RADIUS server has changed to the **Block** state in the RADIUS scheme. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 secondary authentication 10.1.1.11
 secondary accounting 10.1.1.11
 key authentication cipher $c$3$GBZ1jhslcGwSOpSejsESMnOr8Gb8SIT5ew==
 key accounting cipher $c$3$nGb/DWK8pxbHaLXQVc+xsmbUr1etIZVd7Q==
```

```
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

Example: Configuring RADIUS authentication and authorization in ACS for SSH users

Network configuration

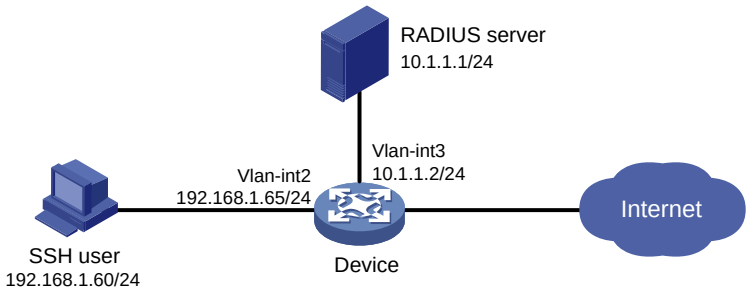
As shown in Figure 10, configure the device to meet the following requirements:

- Act as the Stelnet server to provide RADIUS-based authentication and authorization services for the SSH user.
- Assign the highest level of privilege to the SSH user after the user passes authentication.

The RADIUS server runs Cisco ACS. Add a user account with username **manager@bbb** and password **1234ab##** on the RADIUS server.

The host runs Stelnet client software.

Figure 10 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the RADIUS server to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY user lines.
- To support Stelnet clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the Stelnet server.
- Configure RADIUS authentication and authorization by performing the following tasks on the device:
  - Create a RADIUS scheme.
  - Specify the authentication and authorization servers.
  - Apply the RADIUS scheme to the ISP domain to which the SSH users belong on the device.

- Enable the default user role feature and specify **network-admin** as the default user role, so the authenticated users can obtain the highest level of privilege.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx

Hardware	Software version
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx

Hardware	Software version
IE4520 series	Release 66xx
S5135S-EI	Release 6810 and later versions

Restrictions and guidelines

When you configure RADIUS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring the RADIUS server

In this example, the server runs ACS 4.2. Before you perform the following tasks, make sure the host, the device, and the RADIUS server can reach each other.

1. Enter the username and password, and click **Login**, as shown in Figure 11.

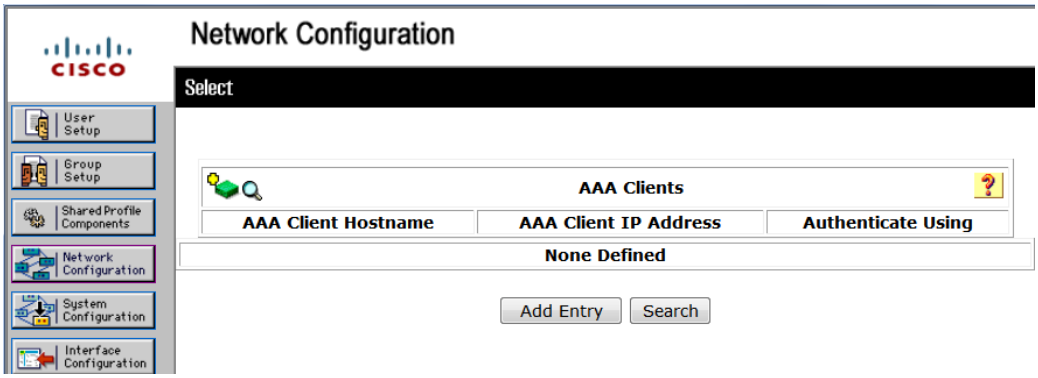
Figure 11 Logging into ACS

2. Add the device to ACS as an AAA client:

a. In the navigation tree, click **Network Configuration**.

b. Click **Add Entry**, as shown in Figure 12.

Figure 12 Adding an AAA client



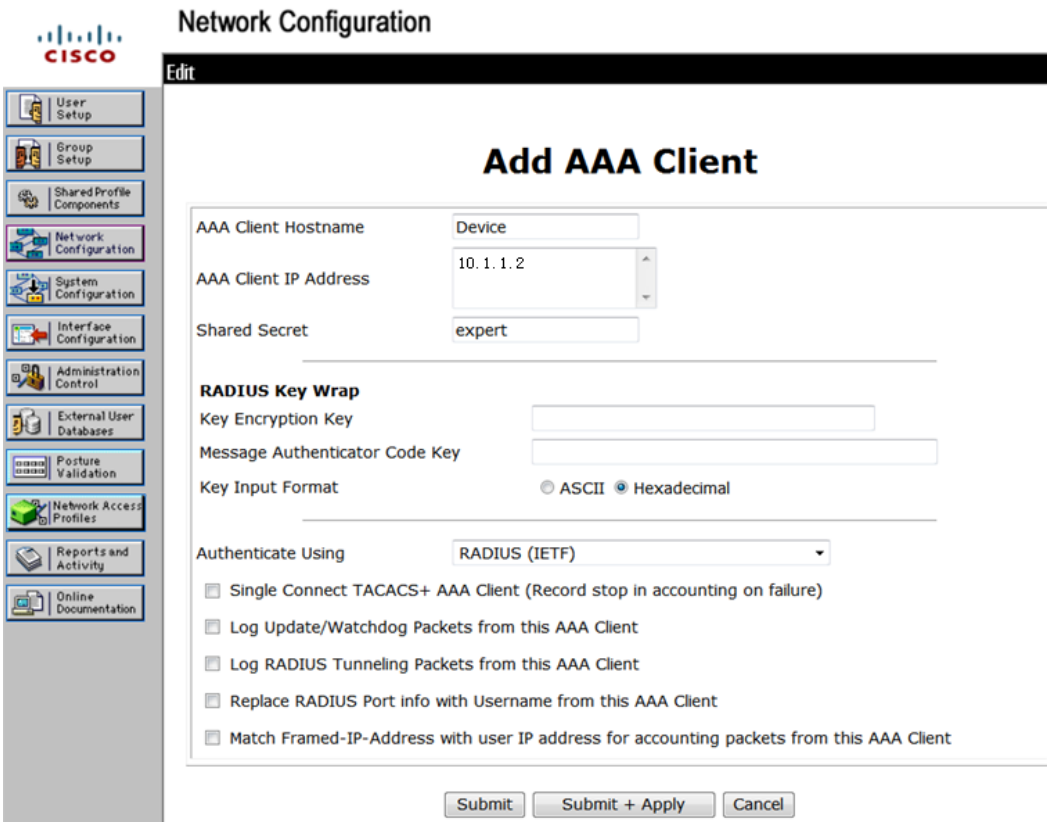
c. On the **Add AAA Client** page, configure the following parameters, as shown in Figure 13:

- Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
- Enter **10.1.1.2** in the **AAA Client IP Address** field.

  The IP address is the source IP address for outgoing RADIUS packets on the device.
- Enter **expert** in the **Shared Secret** field.

  The shared secret must be the same as the authentication and accounting keys configured on the device for secure RADIUS communication.
- Select **RADIUS (IETF)** from the **Authenticate Using** list.

Figure 13 Configuring the AAA client



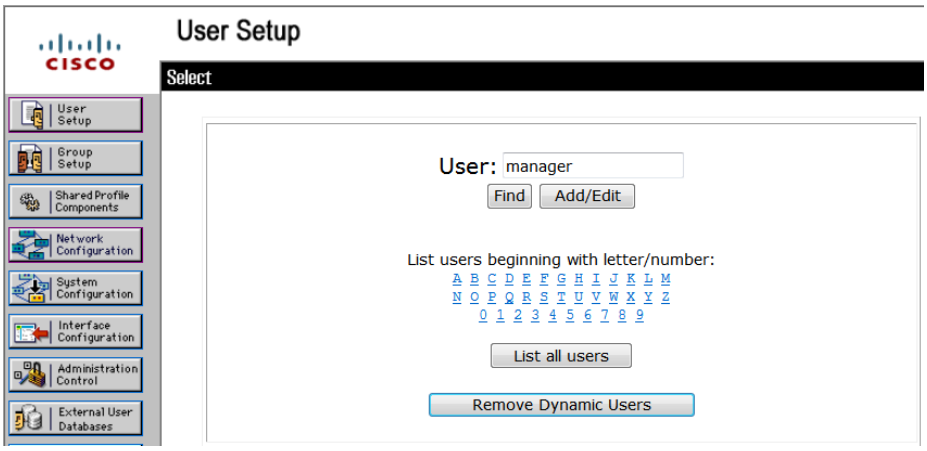
d. Click **Submit + Apply**.

3. Add a user:

a. In the navigation tree, click **User Setup**.

b. On the **User Setup** page, enter **manager** in the **User** field and click **Add/Edit**, as shown in Figure 14.

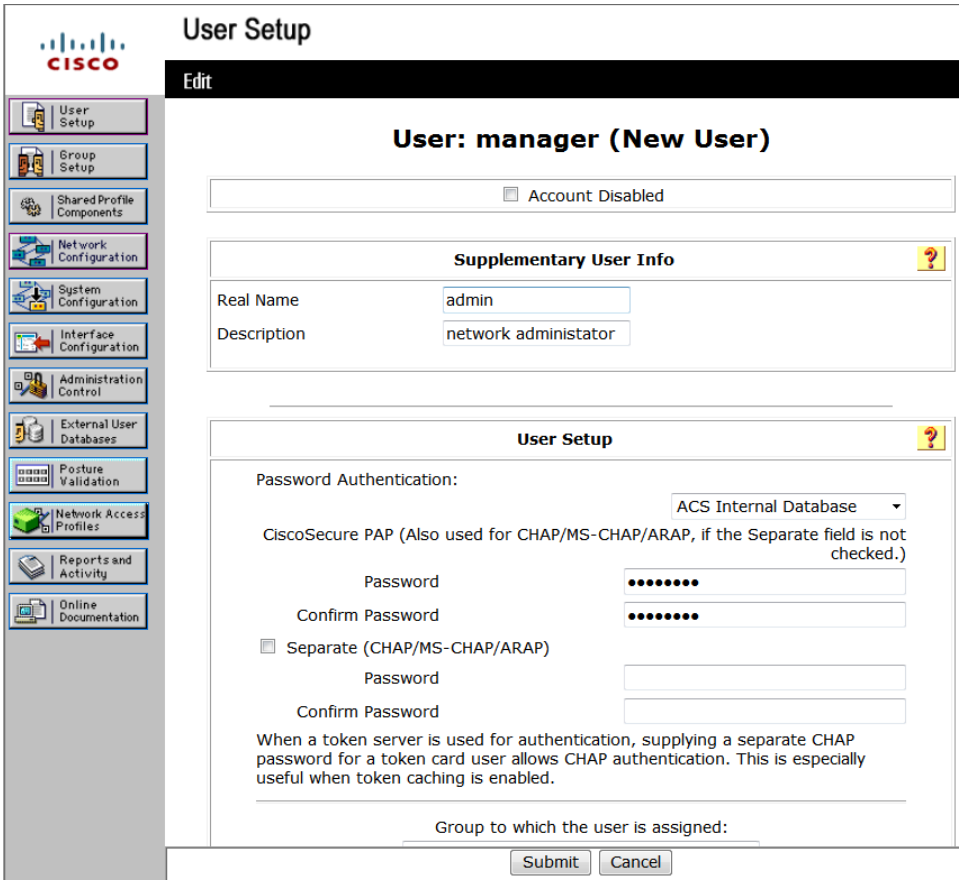
Figure 14 Adding a user



c. Configure parameters for the user, including the user password and user group, as shown in Figure 15.

This example uses the default user group.

Figure 15 Configuring the user manager



d. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.65 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Create a local DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........
Create the key pair successfully.
```

Create a local 256-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

Create a local 384-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Enable the default user role feature and specify **network-admin** as the default user role.

```
[Device] role default-role enable network-admin
```

Create a RADIUS scheme named **rad**.

```
[Device] radius scheme rad
```

Specify the primary RADIUS authentication server with the IP address 10.1.1.1 and port number 1812.

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the shared key as **expert** for secure RADIUS communication between the device and RADIUS server.

```
[Device-radius-rad] key authentication simple expert
```

Remove the domain name from usernames sent to the RADIUS server.

```
[Device-radius-rad] user-name-format without-domain
[Device-radius-rad] quit
```

Create an ISP domain named **bbb**, and specify the domain to use RADIUS scheme **rad** as the authentication and authorization methods of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login none
[Device-isp-bbb] quit
```

Verifying the configuration

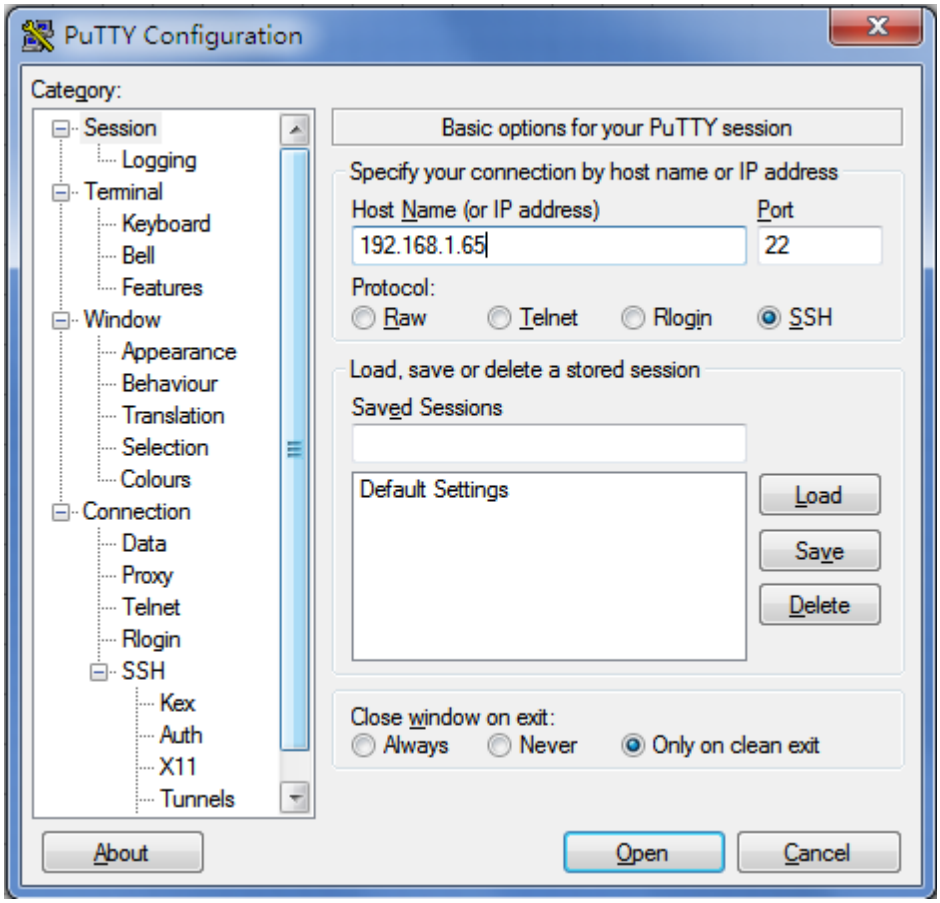
Stelnet client software includes PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY 0.58.

To verify that you can log into the Stelnet server from the Stelnet client:

1. Launch PuTTY.
2. From the navigation tree, click **Session**.

   The **PuTTY Configuration** page appears.
3. Configure the following parameters, as shown in Figure 16:
   a. Enter **192.168.1.65** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Protocol**.

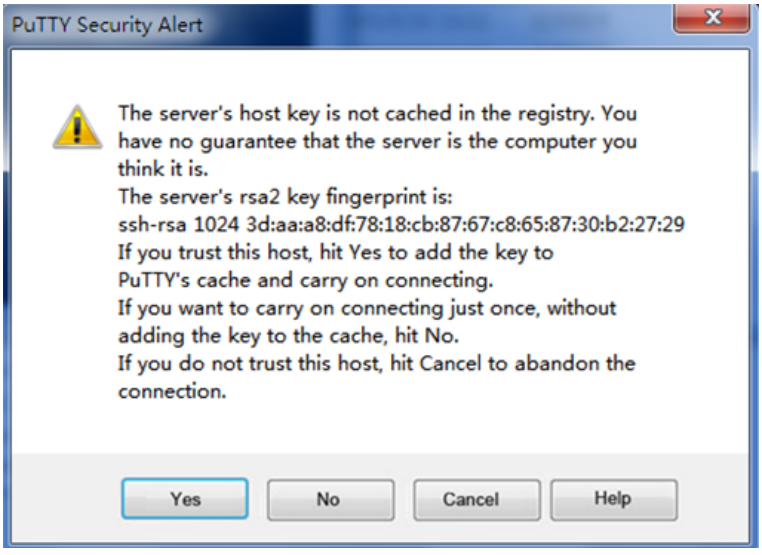
Figure 16 Specifying basic connection parameters



4. Click **Open**.

   The system might display a security alert dialog box, as shown in Figure 17.

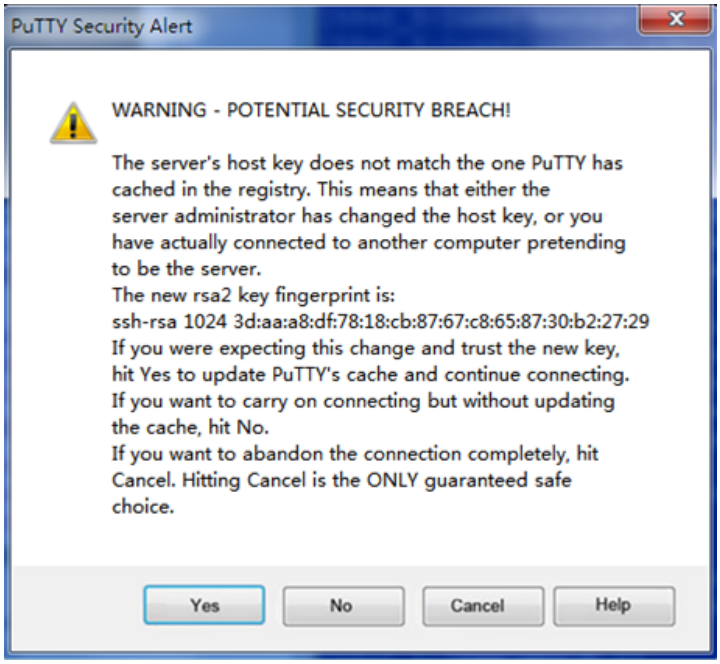
   Figure 17 PuTTY Security Alert dialog box (1)



5. Click **Yes** or **No** to continue the connection.

   The system might display another security alert dialog box, as shown in Figure 18.

Figure 18 PuTTY Security Alert dialog box (2)



6. Click **Yes** or **No** to continue the connection.
7. Enter username **manager@bbb** and password **1234ab##** to log into the Stelnet server.

```
login as: manager@bbb
manager@bbb@192.168.1.65's password:

******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.65 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 key authentication cipher $c$3$+zkawxNT2KQ1IhixdPDszSvNAH5b+yFMIQ==
 user-name-format without-domain
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login none
#
role default-role enable network-admin
#
```

Example: Configuring HWTACACS authentication and authorization in ACS for SSH users

Network configuration

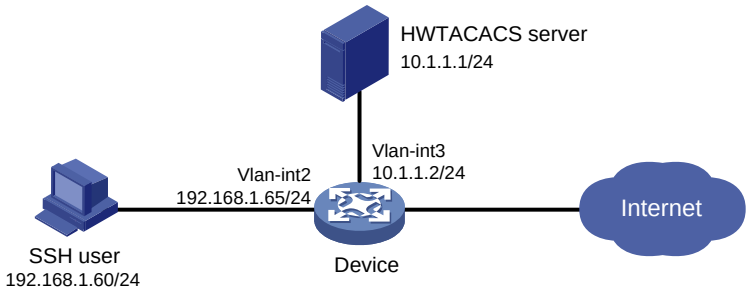
As shown in Figure 19, configure the device to meet the following requirements:

- Act as the Stelnet server to provide HWTACACS-based authentication and authorization services for the SSH user.
- Assign the highest level of privilege to the SSH user after the user passes authentication.

The HWTACACS server runs Cisco ACS. Add a user account with username **manager@bbb** and password **1234ab##** on the HWTACACS server.

The host runs Stelnet client software.

Figure 19 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure the SSH username and password on the HWTACACS server to identify valid users.
- For SSH users to perform AAA, set the authentication mode to **scheme** on VTY user lines.
- To support Stelnet clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the Stelnet server.
- Configure HWTACACS authentication and authorization by performing the following tasks on the device:
  - Create an HWTACACS scheme.
  - Specify the authentication and authorization servers.
  - Apply the HWTACACS scheme to the ISP domain to which the SSH users belong on the device.
- Enable the default user role feature and specify **network-admin** as the default user role, so the authenticated users can have the highest level of privilege.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI series S6520X-EI series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI series S6520-SI series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx

Hardware	Software version
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI	Release 6810 and later versions

Restrictions and guidelines

When you configure HWTACACS authentication and authorization for SSH users, follow these restrictions and guidelines:

- The Stelnet server supports only 256-bit and 384-bit ECDSA key pairs.
- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.

Procedures

Configuring the HWTACACS server

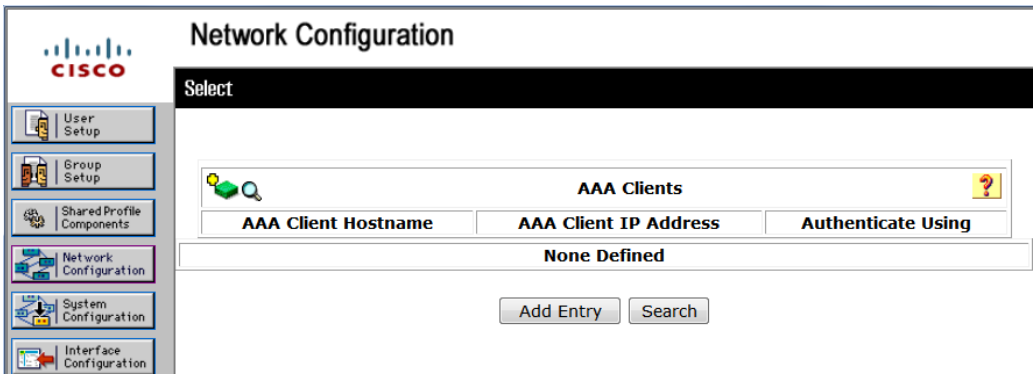
In this example, the server runs ACS 4.2. Before you perform the following tasks, make sure the host, the device, and the HWTACACS server can reach each other.

1. Enter the username and password, and click **Login**, as shown in Figure 20.

Figure 20 Logging into ACS

2. Add the device to ACS as an AAA client:
   a. In the navigation tree, click **Network Configuration**.
   b. Click **Add Entry**, as shown in Figure 21.

Figure 21 Adding an AAA client

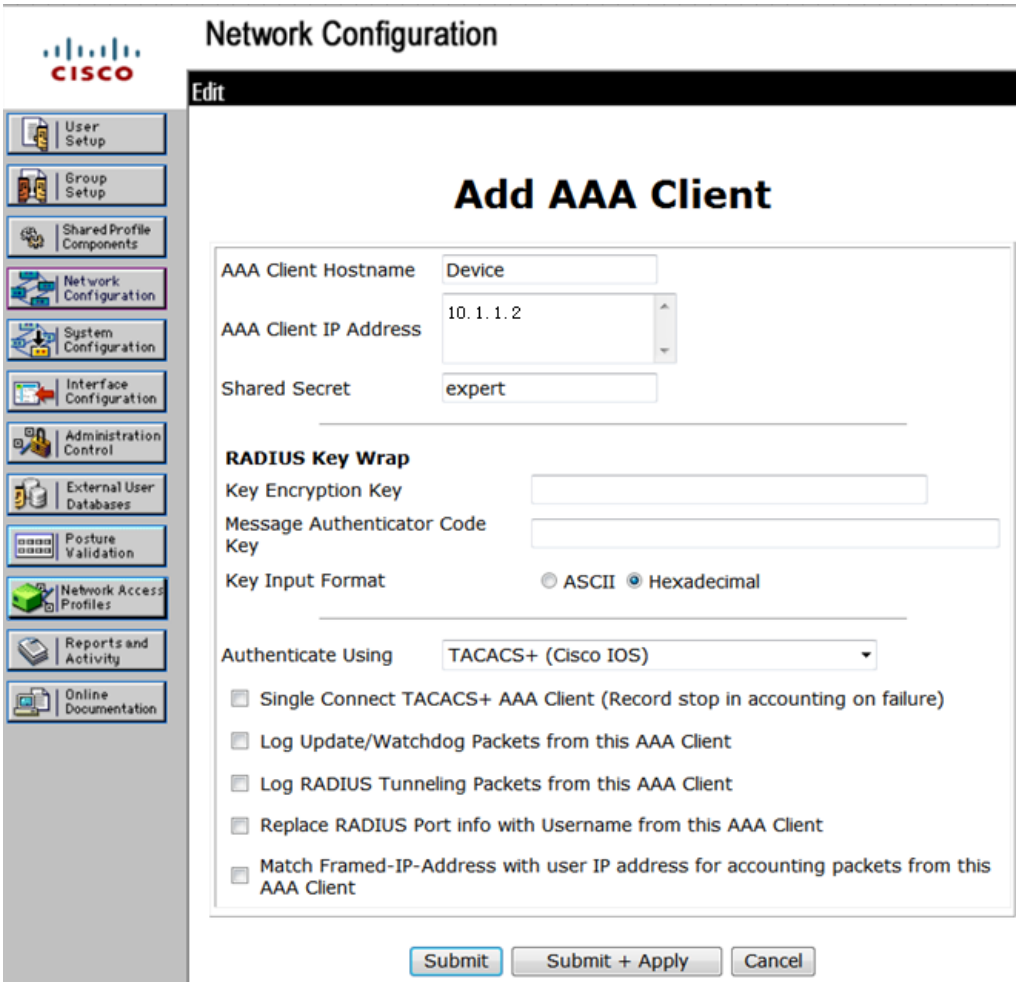


   c. On the **Add AAA Client** page, configure the following parameters, as shown in Figure 22:
      - Enter an AAA client hostname in the **AAA Client Hostname** field. This example uses **Device**.
      - Enter **10.1.1.2** in the **AAA Client IP Address** field.

        The IP address is the source IP address for outgoing HWTACACS packets on the device.
      - Enter **expert** in the **Shared Secret** field.

        The shared secret must be the same as the authentication, authorization, and accounting keys configured on the device for secure HWTACACS communication.
      - Select **TACACS+ (Cisco IOS)** from the **Authenticate Using** list.

Figure 22 Adding an AAA client



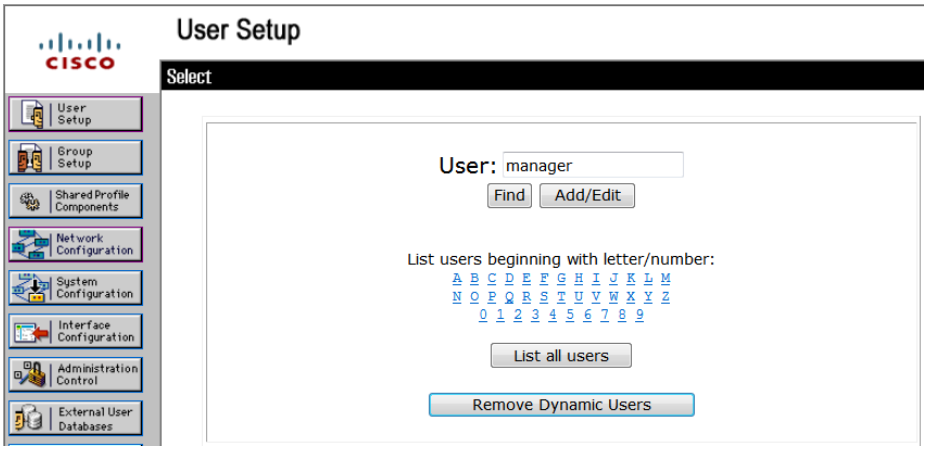
d. Click **Submit + Apply**.

3. Add a user:

a. In the navigation tree, click **User Setup**.

b. On the **User Setup** page, enter **manager** in the **User** field and click **Add/Edit**, as shown in Figure 23.

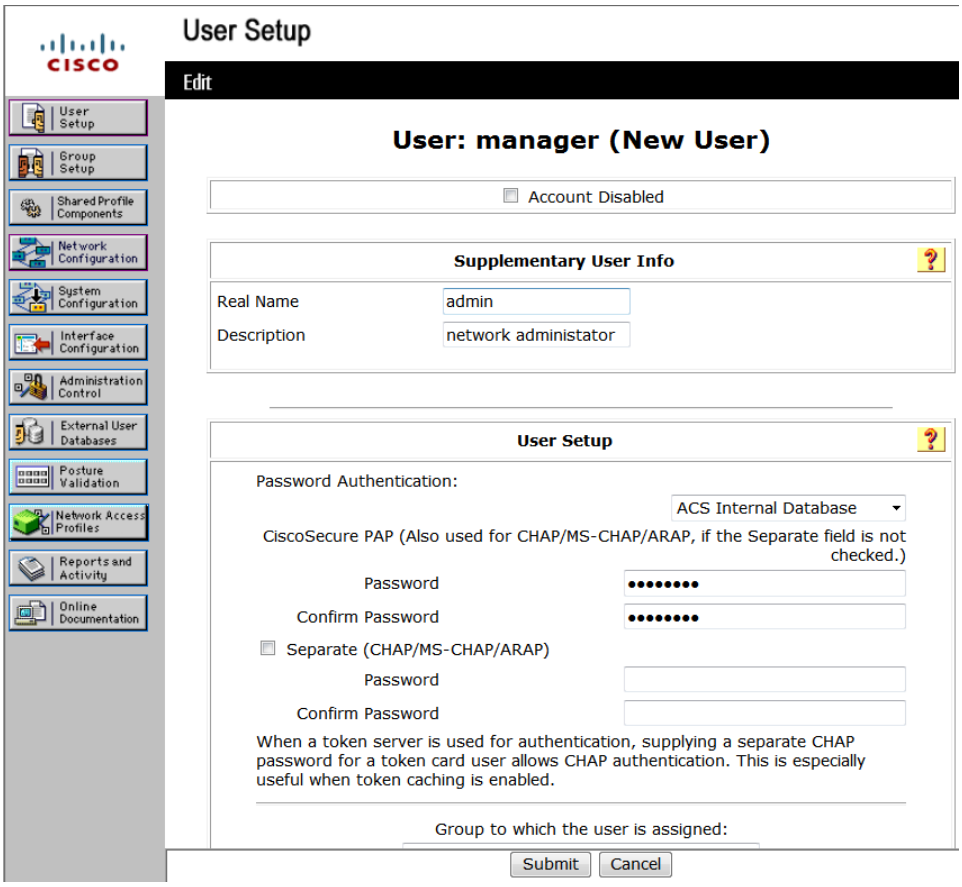
Figure 23 Adding a user



c. Configure parameters for the user, including the user password and user group, as shown in Figure 24.

This example uses the default user group.

Figure 24 Configuring the user manager



d. Click **Submit**.

Configuring the device

Create VLAN 2 and assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.65 255.255.255.0
[Device-Vlan-interface2] quit
```

Create VLAN 3 and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

Assign an IP address to VLAN-interface 3.

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

Create a local RSA key pair.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Create a local DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........
Create the key pair successfully.
```

Create a local 256-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

Create a local 384-bit ECDSA key pair.

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the Stelnet server.

```
[Device] ssh server enable
```

Enable scheme authentication on VTY user lines 0 through 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Enable the default user role feature and specify **network-admin** as the default user role.

```
[Device] role default-role enable network-admin
```

Create an HWTACACS scheme named **tac**.

```
[Device] hwtacacs scheme tac
```

Specify the primary HWTACACS authentication server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-tac] primary authentication 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS authentication server.

```
[Device-hwtacacs-tac] key authentication simple expert
```

Specify the primary HWTACACS authorization server with the IP address 10.1.1.1 and port number 49.

```
[Device-hwtacacs-tac] primary authorization 10.1.1.1 49
```

Specify the shared key as **expert** for secure HWTACACS communication between the device and HWTACACS authorization server.

```
[Device-hwtacacs-tac] key authorization simple expert
```

Remove the domain name from usernames sent to the HWTACACS server.

```
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

Create an ISP domain named **bbb**, and specify the domain to use HWTACACS scheme **tac** for authentication and authorization of login users.

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme tac
[Device-isp-bbb] authorization login hwtacacs-scheme tac
[Device-isp-bbb] accounting login none
[Device-isp-bbb] quit
```

Verifying the configuration

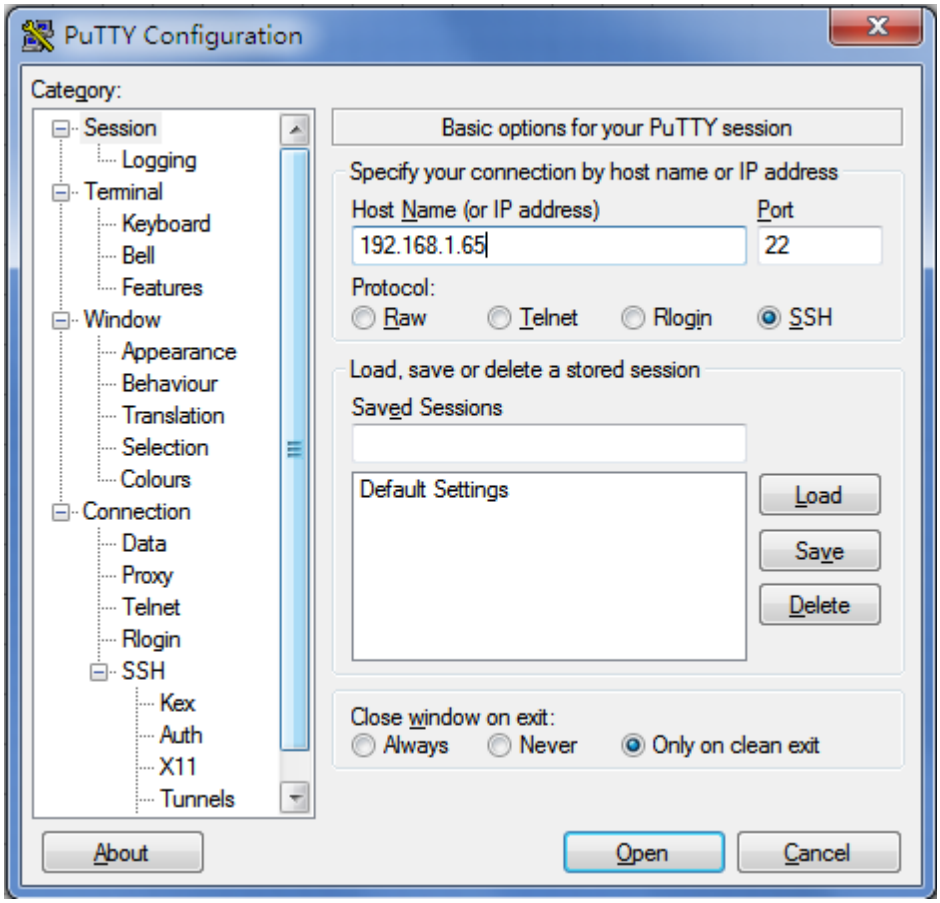
Stelnet client software includes PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY 0.58.

To verify that you can log into the Stelnet server from the Stelnet client:

1. Launch PuTTY.
2. From the navigation tree, click **Session**.

   The **PuTTY Configuration** page appears.
3. Configure the following parameters, as shown in Figure 25:
   a. Enter **192.168.1.65** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Protocol**.

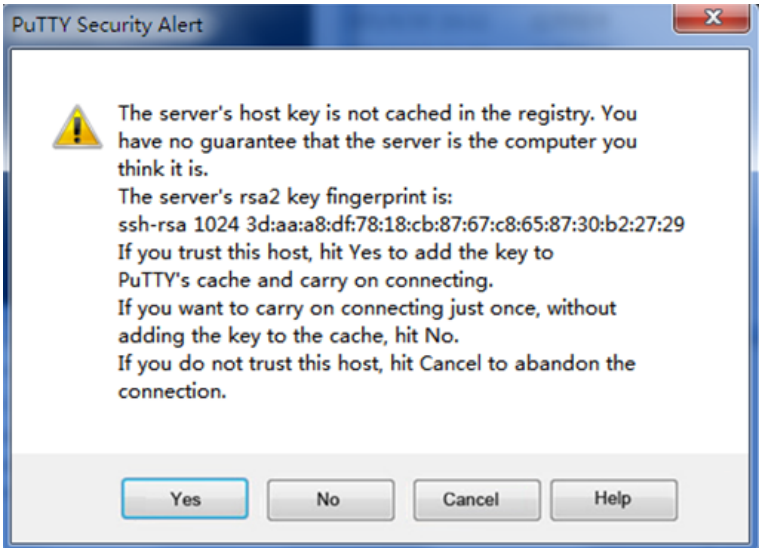
Figure 25 Specifying basic connection parameters



4. Click **Open**.

   The system might display a security alert dialog box, as shown in Figure 26.

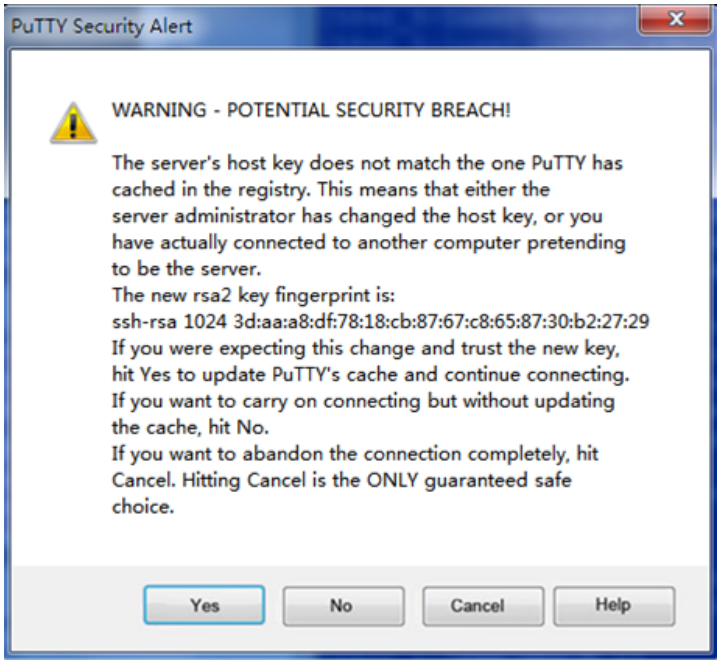
Figure 26 PuTTY Security Alert dialog box (1)



5. Click **Yes** or **No** to continue the connection.

   The system might display another security alert dialog box, as shown in Figure 27.

Figure 27 PuTTY Security Alert dialog box (2)



6. Click **Yes** or **No** to continue the connection.
7. Enter username **manager@bbb** and password **1234ab##** to log into the Stelnet server.

```
login as: manager@bbb
manager@bbb@192.168.1.65's password:

******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.65 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
ssh server enable
#
hwtacacs scheme tac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 key authentication cipher $c$3$/9bCuPjMxjOtUvBx8NjtN+AnAsuLT2SrNA==
 key authorization cipher $c$3$QF/fFJNv9IyKyFlsNOpeBYnDXArNhOvOdQ==
 user-name-format without-domain
#
domain bbb
 authentication login hwtacacs-scheme tac
 authorization login hwtacacs-scheme tac
 accounting login none
#
role default-role enable network-admin
#
```

Contents

Introduction

This document provides port security configuration examples.

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. The feature provides the following functions:

- Prevents unauthorized access to a network by checking the source MAC address of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC address of outbound traffic.
- Controls MAC address learning and authentication on a port to make sure the port learns only source trusted MAC addresses.

Port security supports the following categories of security modes:

- **MAC learning control**—Includes two modes: autoLearn and secure. MAC address learning is permitted on a port in autoLearn mode and disabled in secure mode.
- **Authentication**—Security modes in this category implement MAC authentication, 802.1X authentication, or a combination of these two authentication methods.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of port security.

General restrictions and guidelines

When you configure port security, follow these restrictions and guidelines:

- Disable global 802.1X and MAC authentications before you enable port security on a port.
- Port security automatically modifies the following 802.1X or MAC authentication settings for different security modes:
  - The status of 802.1X and MAC authentication.
  - The 802.1X access control method.
  - The 802.1X port authorization state.
- Disabling port security on a port will log off all online users on that port.
- Port security modes are mutually exclusive with link aggregation and service loopback group.
- The maximum number of users a port supports equals the smaller value from the following values:
  - The maximum number of secure MAC addresses that port security allows.
  - The maximum number of concurrent users the authentication mode in use allows.

  For example, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode, port security's limit takes effect.
- To change the security mode of a port security-enabled port, you must use the **undo `port-security port-mode`** command to set the port in noRestrictions mode first.

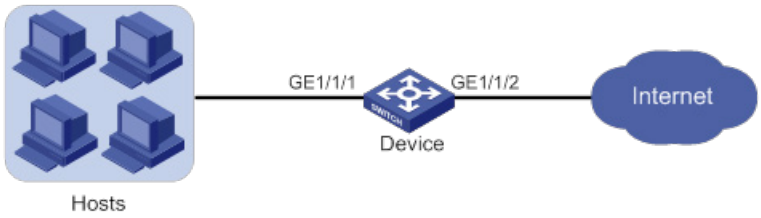
Example: Configuring autoLearn mode

Network configuration

As shown in Figure 1:

- Configure port security mode **autoLearn** on GigabitEthernet 1/0/1 to allow users to access the network without authentication.
- Configure the port to accept a maximum of 64 users (secure MAC addresses) to access the network. After the number of secure MAC addresses reaches 64, the port stops learning secure MAC addresses and no new user can access the network.
- To prevent inactive users from using secure MAC address entries, configure a secure MAC address aging timer.
- Configure GigabitEthernet 1/0/1 to shut down temporarily for 30 seconds when a new user accesses the network after the number of secure MAC addresses reaches 64.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx

Hardware	Software version
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch	Release 63xx

Hardware	Software version
E152C switch E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

Before you enable the autoLearn mode, you must set the maximum number of secure MAC addresses that port security allows on the port (by using the **`port-security max-mac-count`** command). You cannot change the setting after the port is set to the **autoLearn** mode.

Procedures

Enable port security.

```
<Device> system-view
[Device] port-security enable
```

Set the secure MAC aging timer to 30 minutes.

```
[Device] port-security timer autolearn aging 30
```

Set port security's limit on the number of secure MAC addresses to 64 on GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to **autoLearn**.

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Specify the intrusion protection action as **disableport-temporarily**.

```
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet1/0/1] quit
```

Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Device] port-security timer disableport 30
```

Verifying the configuration

Verify that port security is correctly configured.

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Disabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   Traffic-statistics     : Disabled
   OUI value list         :

 GigabitEthernet1/0/1 is link-up
   Port mode                       : autoLearn
   NeedToKnow mode                 : Disabled
   Intrusion protection mode       : DisablePortTemporarily
   Security MAC address attribute
       Learning mode               : Sticky
       Aging type                  : Periodical
   Max secure MAC addresses        : 64
   Current secure MAC addresses    : 5
   Authorization                   : Permitted
   NAS-ID profile                  : Not configured
   Free VLANs                      : Not configured
   Open authentication             : Disabled
   MAC-move VLAN check bypass      : Disabled
```

The port performs MAC address learning, and you can view the number of learned MAC addresses in the **Current secure MAC addresses** field.

Display information about the learned MAC addresses.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security intrusion-mode disableport-temporarily
```

```
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 00e0-fc00-5920 vlan 1
 port-security mac-address security sticky 00e0-fc00-592a vlan 1
 port-security mac-address security sticky 00e0-fc00-592b vlan 1
 port-security mac-address security sticky 00e0-fc00-592c vlan 1
 port-security mac-address security sticky 00e0-fc00-592d vlan 1
#
```

Verify that the port security mode changes to **secure** after the number of MAC addresses learned by the port reaches 64.

```
[Device] display port-security interface gigabitethernet 1/0/1
```

Verify that the port is disabled after it receives a frame with an unknown MAC address.

```
[Device] display interface gigabitethernet 1/0/1
```

Verify that the interface is re-enabled after 30 seconds.

```
[Device] display interface gigabitethernet 1/0/1
```

Delete several secure MAC addresses.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] undo port-security mac-address security sticky
00e0-fc00-5920 vlan 1
[Device-GigabitEthernet1/0/1] undo port-security mac-address security sticky
00e0-fc00-592a vlan 1
...
```

Verify that the port security mode changes to **autoLearn** and the port can learn MAC addresses again. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 port-security enable
 port-security timer disableport 30
 port-security timer autolearn aging 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security intrusion-mode disableport-temporarily
 port-security max-mac-count 64
 port-security port-mode autolearn
#
```

Example: Configuring userLoginWithOUI mode

Network configuration

As shown in Figure 2:

- An 802.1X user on a host and a printer are attached to port GigabitEthernet 1/0/1 on the device.
- The device uses a RADIUS server (IMC in this example) to perform authentication, authorization, and accounting for all users in ISP domain **sun**.
- The device and the server use the shared key **expert** for secure RADIUS communication.

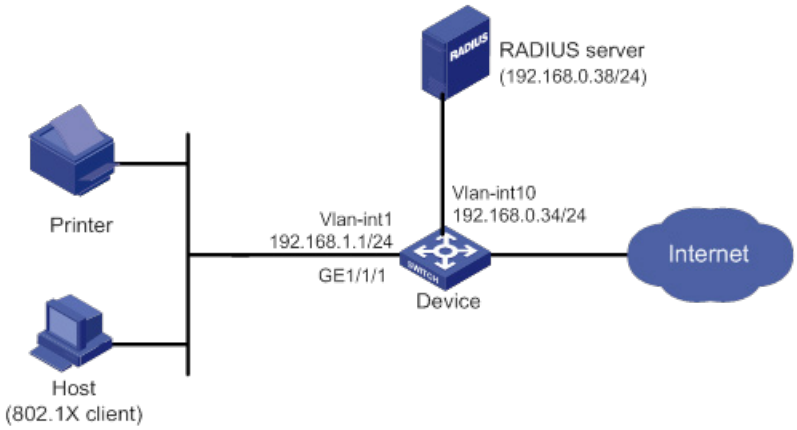
Configure port security mode **userLoginWithOUI** on port GigabitEthernet 1/0/1 to meet the following requirements:

- Permit only one 802.1X user to pass authentication.
- Permit the printer to access the Internet.

For the printer to pass authentication, add its OUI to the OUI list of port security.

Configure the **blockmac** intrusion protection action on GigabitEthernet 1/0/1, so the device adds the source MAC addresses of illegal frames to the blocked MAC address list. The device discards all frames sourced from the blocked MAC addresses.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and	Release 63xx

Hardware	Software version
S5120V3-54P-PWR-SI switches)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Configuring the RADIUS server

This example uses IMC PLAT 7.0 (E0201) and IMC UAM 7.0 (E0201) to describe the procedure.

1. Add the device to IMC as an access device:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Device Management** > **Access Device**.

c. Click **Add**.

   The **Add Access Device** page opens.

d. In the **Access Configuration** area, configure the following parameters:

   - Enter **1812** in the **Authentication Port** field, and enter **1813** in the **Accounting Port** field.
   - Select **LAN Access Service** from the **Service Type** list.
   - Select **HP(Comware)** from the **Access Device Type** list.
   - Enter **expert** in the **Shared Key** and **Confirm Shared Key** field.
   - Use the default values for other parameters.

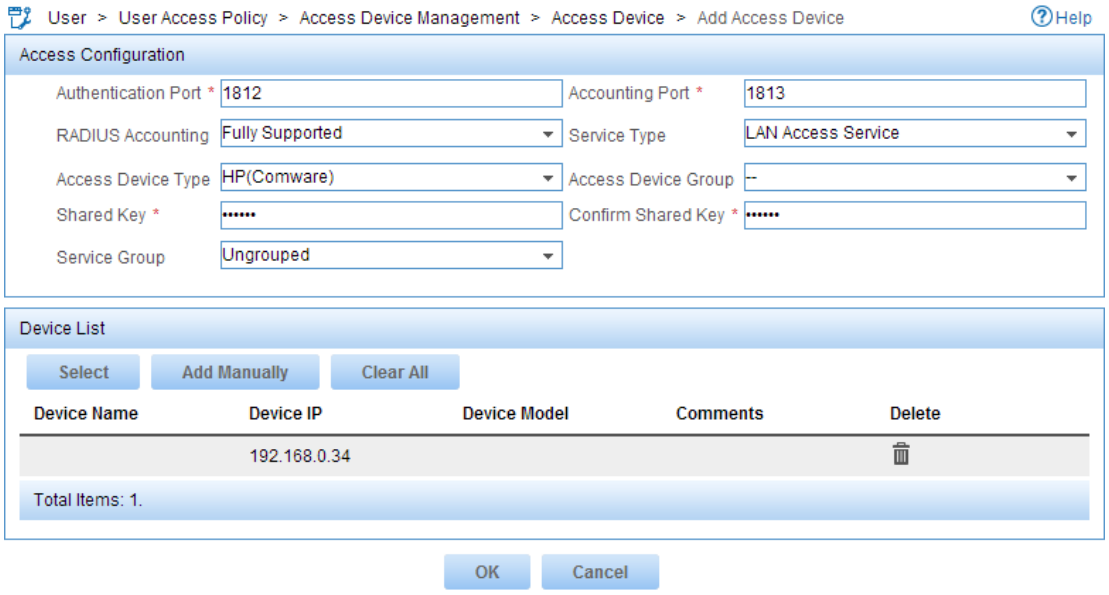
e. In the **Device List** area, click **Select** or **Add Manually** to add the device at **192.168.0.34** as an access device.

   You must specify the source IP address of outgoing RADIUS packets on the device as the IP address of the access device on the server.

   On the device, the source IP address is configured by using the **`nas-ip`** or **`radius nas-ip`** command. The IP address configured by using the **`nas-ip`** command has a higher priority than the IP address configured by using the **`radius nas-ip`** command. If no IP address is specified as the source IP address, the IP address of the packet outbound interface is used as the source IP address. In this example, the IP address of the packet outbound interface is used, which is 192.168.0.34.

f. Click **OK**.

Figure 3 Adding the device as an access device



2. Add an access policy:

   a. Click the **User** tab.

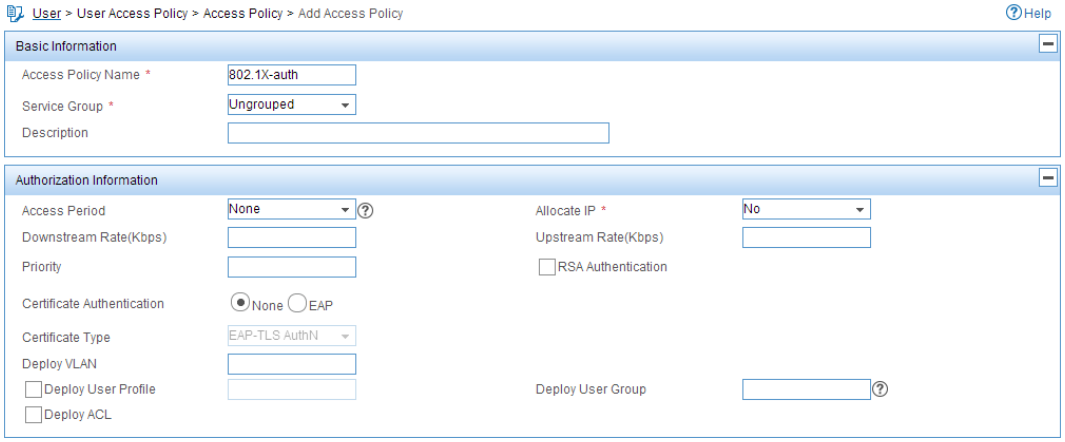
   b. From the navigation tree, select **User Access Policy** > **Access Policy**.

   c. Click **Add**.

   d. On the page that opens, configure the following parameters, as shown in Figure 4:

      - Enter **802.1X-auth** in the **Access Policy Name** field.
      - Use the default values for other parameters.

Figure 4 Adding an access policy



e. Click **OK**.

3. Add an access service:

a. Click the **User** tab.

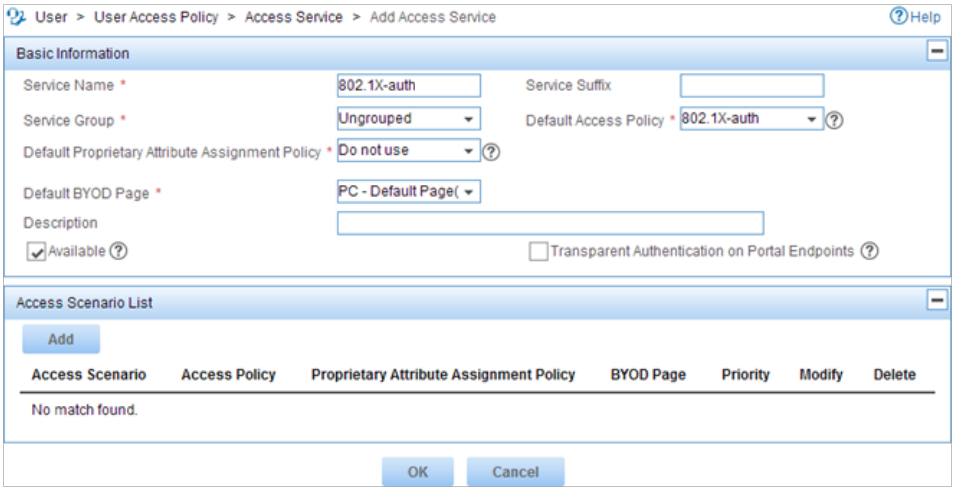
b. From the navigation tree, select **User Access Policy** > **Access Service**.

c. Click **Add**.

d. On the page that opens, configure the following parameters, as shown in Figure 5:

- Enter **802.1X-auth** in the **Service Name** field.
- Select **802.1X-auth** from the **Default Access Policy** list.

Figure 5 Adding an access service



e. Click **OK**.

4. Add an access user:

a. Click the **User** tab.

b. From the navigation tree, select **Access User Management** > **All Access Users**.

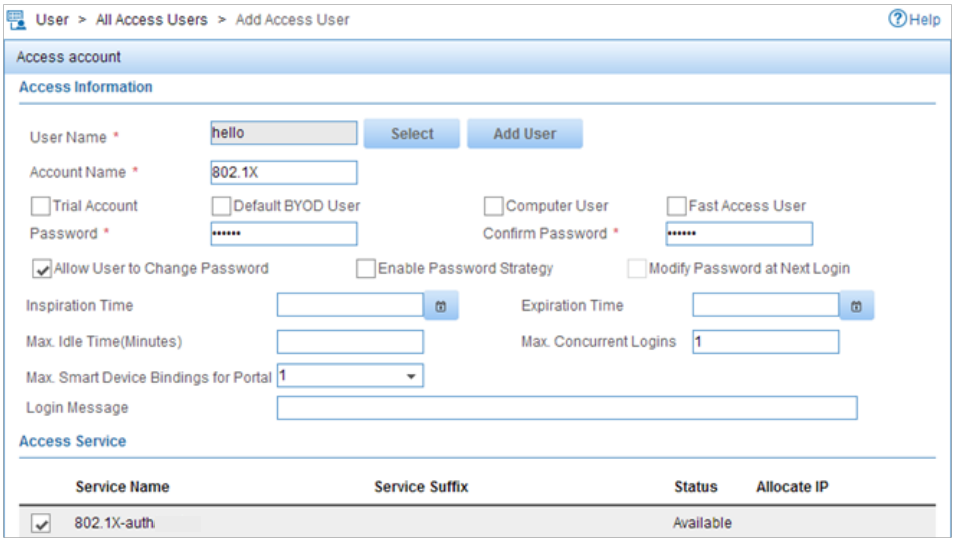
c. Click **Add**.

d. On the **Add Access User** page, configure the following parameters, as shown in Figure 6:

- Click **Select** or **Add User** to associate the user with IMC Platform user **hello**.
- Enter **802.1X** in the **Account Name** field.
- Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.

- Configure other parameters in the **Access Information** area as needed.
- Select **802.1X-auth** from the **Access Service** list.

Figure 6 Adding an access user account



e. Click **OK**.

Configuring the device

The following procedure contains RADIUS commands. For more information about RADIUS commands, see AAA commands in the security command reference for the device.

1. Assign an IP address to each interface, as shown in Figure 2. Make sure the host, printer, device, and RADIUS server can reach each other. (Details not shown.)

2. Configure the RADIUS scheme:

Create RADIUS scheme **radsun**.

```
<Device> system-view
[Device] radius scheme radsun
New RADIUS scheme.
```

Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

```
[Device-radius-radsun] primary authentication 192.168.0.38
```

Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

```
[Device-radius-radsun] primary accounting 192.168.0.38
```

Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key authentication simple expert
```

Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key accounting simple expert
```

Set the response timeout time of the RADIUS server to 5 seconds.

```
[Device-radius-radsun] timer response-timeout 5
```

Set the maximum number of RADIUS packet retransmission attempts to 5.

```
[Device-radius-radsun] retry 5
```

Set the real-time accounting interval to 15 minutes.

```
[Device-radius-radsun] timer realtime-accounting 15
```

Exclude domain names from the usernames sent to the RADIUS server.

```
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
```

Create ISP domain **sun** and enter ISP domain view.

```
[Device] domain sun
```

Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication, authorization, and accounting of all LAN users.

```
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

Configure domain **sun** as the default domain.

```
[Device] domain default enable sun
```

3. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

```
[Device] dot1x authentication-method chap
```

4. Configure port security:

Add five OUI values, including the OUI of the printer. You can add a maximum of 16 OUI values. If the MAC address of a user matches one of the OUIs, the device will allow the user to pass authentication. Each port can permit only one OUI user to pass authentication.

```
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
```

Set the port security mode to **userLoginWithOUI**.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

Configure port GigabitEthernet 1/0/1 to perform the **blockmac** intrusion protection action.

```
[Device-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
[Device-GigabitEthernet1/0/1] quit
```

Enable port security.

```
[Device] port-security enable
```

Verifying the configuration

Display RADIUS scheme **radsun**.

In Release 63xx:

```
[Device] display radius scheme radsun
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radsun
  Index: 0
  Primary authentication server:
    Host name: Not configured
    IP   : 192.168.0.38                          Port: 1812
    VPN  : Not configured
```

```
    State: Active
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
    Host name: Not configured
    IP   : 192.168.0.38                          Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Accounting-On function                    : Disabled
    extended function                       : Disabled
    retransmission times                    : 50
    retransmission interval(seconds)        : 3
  Timeout Interval(seconds)                 : 5
  Retransmission Times                      : 5
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)              : 5
  Realtime Accounting Interval(seconds)     : 900
  Stop-accounting packets buffering         : Enabled
    Retransmission times                    : 500
  NAS IP Address                            : Not configured
  VPN                                       : Not configured
  User Name Format                          : without-domain
  Data flow unit                            : Byte
  Packet unit                               : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                              : Standard
  Attribute Remanent-Volume unit            : Kilo
  server-load-sharing                       : Disabled
  Attribute 31 MAC format                   : HH-HH-HH-HH-HH-HH
  Stop-accounting-packet send-force         : Disabled
  Reauthentication server selection         : Reselect
------------------------------------------------------------------
```

In Release 65xx:

```
[Device] display radius scheme radsun
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radsun
  Index: 0
  Primary authentication server:
    Host name: Not configured
    IP   : 192.168.0.38                          Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
```

```
    Host name: Not configured
    IP   : 192.168.0.38                          Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Accounting-On function                    : Disabled
    extended function                       : Disabled
    retransmission times                    : 50
    retransmission interval(seconds)        : 3
  Timeout Interval(seconds)                 : 5
  Retransmission Times                      : 5
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)              : 5
  Realtime Accounting Interval(seconds)     : 900
  Stop-accounting packets buffering         : Enabled
    Retransmission times                    : 500
  NAS IP Address                            : Not configured
  VPN                                       : Not configured
  User Name Format                          : without-domain
  Data flow unit                            : Byte
  Packet unit                               : One
  Attribute 15 check-mode                   : Strict
  Attribute 25                              : Standard
  Attribute Remanent-Volume unit            : Kilo
  server-load-sharing                       : Disabled
  Attribute 30 format                       : HH-HH-HH-HH-HH-HH:SSID
  Attribute 30 MAC format                   : HH-HH-HH-HH-HH-HH
  Attribute 31 MAC format                   : HH-HH-HH-HH-HH-HH
  Stop-accounting-packet send-force         : Disabled
  Reauthentication server selection         : Reselect
  Attribute 218 of vendor ID 25506          : DHCP-Option 61
                                              Format 1 (1-byte Type field)
------------------------------------------------------------------------
```

Display the port security configuration on GigabitEthernet 1/0/1.

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
   Intrusion trap         : Disabled
   Address-learned trap   : Disabled
```

```
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
  Open authentication    : Disabled
  Traffic-statistics     : Disabled
  OUI value list         :
      Index :  1       Value : 123401
      Index :  2       Value : 123402
      Index :  3       Value : 123403
      Index :  4       Value : 123404
      Index :  5       Value : 123405

 GigabitEthernet1/0/1 is link-up
  Port mode                      : userLoginWithOUI
  NeedToKnow mode                : Disabled
  Intrusion protection mode      : NoAction
  Security MAC address attribute
      Learning mode              : Sticky
      Aging type                 : Periodical
  Max secure MAC addresses       : Not configured
  Current secure MAC addresses   : 0
  Authorization                  : Permitted
  NAS-ID profile                 : Not configured
  Free VLANs                     : Not configured
  Open authentication            : Disabled
  MAC-move VLAN check bypass     : Disabled
```

After the 802.1X user comes online, the number of secure MAC addresses on the port is 1.

Display 802.1X information.

```
[Device] display dot1x interface gigabitethernet 1/0/1
```

Verify that GigabitEthernet 1/0/1 allows a user whose MAC address has an OUI from the specified OUIs to pass authentication.

```
[Device] display mac-address interface gigabitethernet 1/0/1
MAC Address      VLAN ID    State            Port/NickName            Aging
1234-0300-0011  1            Learned         XGE1/0/1                  Y
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 port-security enable
 port-security oui index 1 mac-address 1234-0100-0000
 port-security oui index 2 mac-address 1234-0200-0000
 port-security oui index 3 mac-address 1234-0300-0000
 port-security oui index 4 mac-address 1234-0400-0000
 port-security oui index 5 mac-address 1234-0500-0000
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
port-security port-mode userlogin-withoui
port-security intrusion-mode blockmac
#
radius scheme radsun
 primary authentication 192.168.0.38
 primary accounting 192.168.0.38
 key authentication cipher $c$3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
 key accounting cipher $c$3$UaUPGk8AfZAQLHFlbKNcEoM2HXGiuWowBQ==
 retry 5
 timer response-timeout 5
 timer realtime-accounting 15
 user-name-format without-domain
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access radius-scheme radsun
#
domain default enable sun
#
```

Example: Configuring macAddressElseUserLoginSecure mode

Network configuration

As shown in Figure 7:

- Users on hosts are attached to port GigabitEthernet 1/0/1 on the device.
- All MAC authentication users use a shared user account with username **aaa** and password **123456TESTplat&!**.
- The device uses a RADIUS server (IMC in this example) to perform authentication, authorization, and accounting for all users in domain **sun**.
- The device and the server use shared key **expert** for secure RADIUS communication.

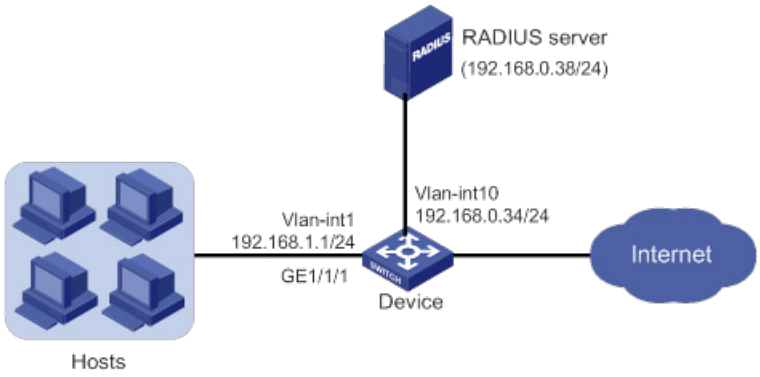
Configure port security mode **macAddressElseUserLoginSecure** on port GigabitEthernet 1/0/1 to meet the following requirements:

- Allow only one 802.1X user to pass authentication, and allow multiple MAC authentication users to pass authentication.
- MAC authentication has a higher priority than 802.1X authentication. For an 802.1X user, the device initiates MAC authentication first, and then 802.1X authentication if the user fails MAC authentication. For a MAC authentication user, the device initiates only MAC authentication.

Configure port GigabitEthernet 1/0/1 to accept a maximum of 64 authenticated users.

Set the NTK mode to **ntkonly** mode on port GigabitEthernet 1/0/1 to prevent outbound frames from being sent to unknown MAC addresses.

Figure 7 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx

Hardware	Software version
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

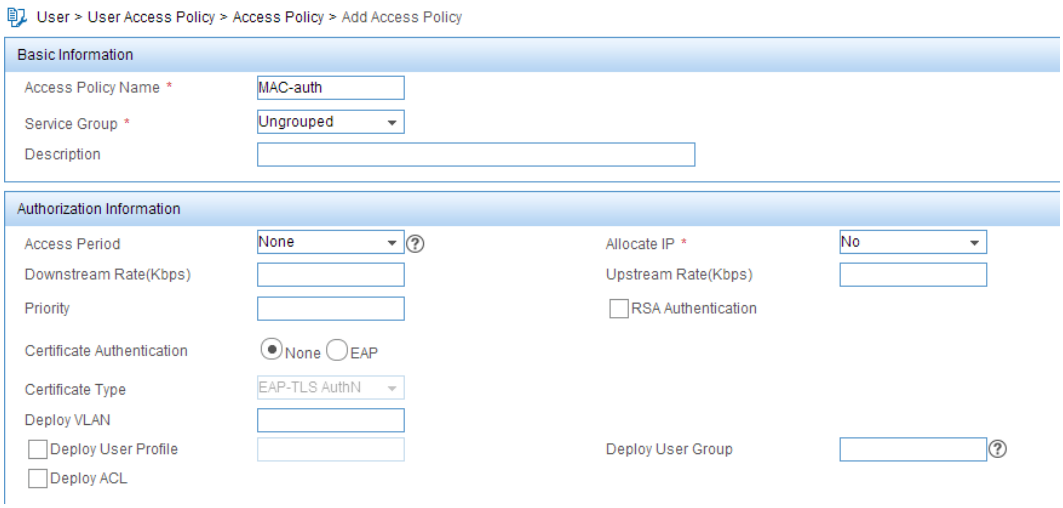
Procedures

Configuring the RADIUS server

This example uses IMC PLAT 7.0 (E0201) and IMC UAM 7.0 (E0201) to describe the procedure.

1. Add the device to IMC as an access device in the same way the device is added to IMC in "Example: Configuring userLoginWithOUI mode."
2. Add an access policy, an access service, and an access user for 802.1X authentication in the same way they are added in "Example: Configuring userLoginWithOUI mode."
3. Add an access policy for MAC authentication:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Policy**.
   c. Click **Add**.
   d. On the page that opens, configure the following parameters, as shown in Figure 8:
      – Enter **MAC-auth** in the **Access Policy Name** field.
      – Use the default values for other parameters.

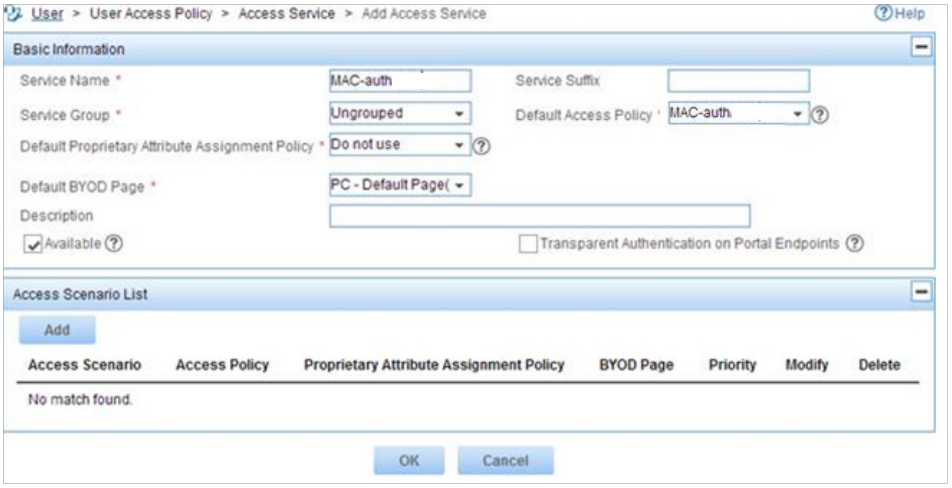
Figure 8 Adding an access policy



e. Click **OK**.

4. Add an access service for MAC authentication:
   a. Click the **User** tab.
   b. From the navigation tree, select **User Access Policy** > **Access Service**.
   c. Click **Add**.
   d. On the page that opens, configure the following parameters, as shown in Figure 9:
      – Enter **MAC-auth** in the **Service Name** field.
      – Select **MAC-auth** from the **Default Access Policy** list.

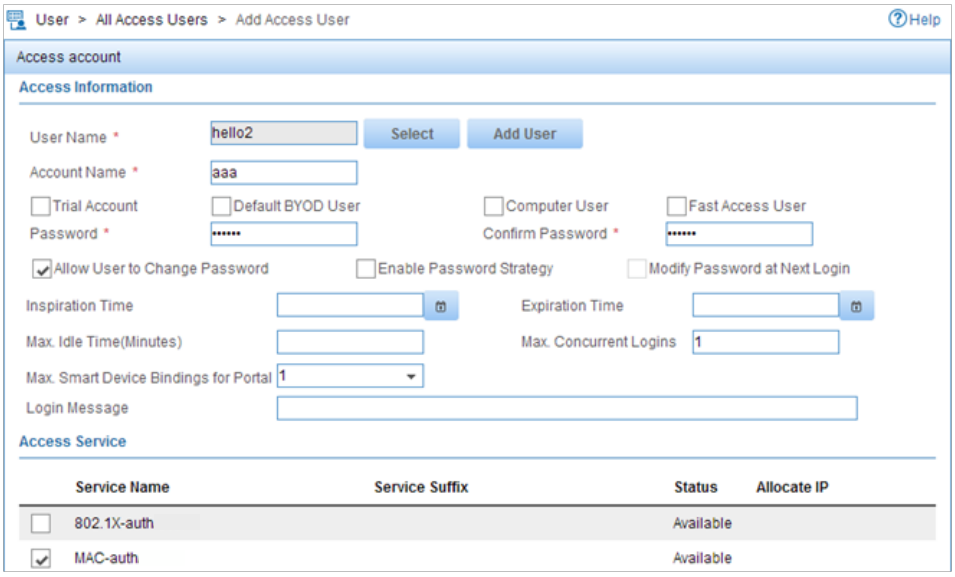
Figure 9 Adding an access service



   e. Click **OK**.

5. Add an access user for MAC authentication:
   a. Click the **User** tab.
   b. From the navigation tree, select **Access User Management** > **All Access Users**.
   c. Click **Add**.
   d. On the **Add Access User** page, configure the following parameters, as shown in Figure 10:
      – Click **Select** or **Add User** to associate the user with IMC Platform user **hello2**.
      – Enter **aaa** in the **Account Name** field.
      – Enter **123456TESTplat&!** in the **Password** and **Confirm Password** fields.
      – Configure other parameters in the **Access Information** area as needed.
      – Select **MAC-auth** from the **Access Service** list.

Figure 10 Adding an access user account



e. Click **OK**.

Configuring the device

1. Assign an IP address to each interface, as shown in Figure 7. Make sure the hosts, device, and RADIUS server can reach each other. (Details not shown.)
2. Configure the RADIUS scheme:

   # Create RADIUS scheme **radsun**.

   ```
   <Device> system-view
   [Device] radius scheme radsun
   New RADIUS scheme.
   ```

   # Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

   ```
   [Device-radius-radsun] primary authentication 192.168.0.38
   ```

   # Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

   ```
   [Device-radius-radsun] primary accounting 192.168.0.38
   ```

   # Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

   ```
   [Device-radius-radsun] key authentication simple expert
   ```

   # Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

   ```
   [Device-radius-radsun] key accounting simple expert
   ```

   # Set the response timeout time of the RADIUS server to 5 seconds.

   ```
   [Device-radius-radsun] timer response-timeout 5
   ```

   # Set the maximum number of RADIUS packet retransmission attempts to 5.

   ```
   [Device-radius-radsun] retry 5
   ```

   # Set the real-time accounting interval to 15 minutes.

   ```
   [Device-radius-radsun] timer realtime-accounting 15
   ```

   # Exclude domain names from the usernames sent to the RADIUS server.

   ```
   [Device-radius-radsun] user-name-format without-domain
   [Device-radius-radsun] quit
   ```

Create ISP domain **sun** and enter ISP domain view.

```
[Device] domain sun
```

Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication, authorization, and accounting of all LAN users.

```
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

Specify ISP domain **sun** as the default domain.

```
[Device] domain default enable sun
```

3. Configure MAC authentication:

Configure a shared account for MAC authentication users, and set the username to **aaa** and password to plaintext string of **123456TESTplat&!**.

```
[Device] mac-authentication user-name-format fixed account aaa password simple
123456TESTplat&!
```

Specify domain **sun** as the global MAC authentication domain.

```
[Device] mac-authentication domain sun
```

4. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

```
[Device] dot1x authentication-method chap
```

5. Configure port security:

Set port security's limit on the number of secure MAC addresses to 64 on GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to **macAddressElseUserLoginSecure**.

```
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

Set the NTK mode of the port to **ntkonly**.

```
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet1/0/1] quit
```

Enable port security.

```
[Device] port-security enable
```

Verifying the configuration

Verify that port security is correctly configured.

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 30 min
   Disableport timeout    : 30 s
   Blockmac timeout       : 180 s
   MAC move               : Denied
   Authorization fail     : Online
   NAS-ID profile         : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap       : Disabled
   Dot1x-logoff trap      : Disabled
```

```
  Intrusion trap         : Disabled
  Address-learned trap   : Disabled
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
  Open authentication    : Disabled
  Traffic-statistics     : Disabled
  OUI value list         :

GigabitEthernet1/0/1 is link-up
  Port mode                      : macAddressElseUserLoginSecure
  NeedToKnow mode                : NeedToKnowOnly
  Intrusion protection mode      : DisablePortTemporarily
  Security MAC address attribute
      Learning mode              : Sticky
      Aging type                 : Periodical
  Max secure MAC addresses       : 64
  Current secure MAC addresses   : 0
  Authorization                  : Permitted
  NAS-ID profile                 : Not configured
  Free VLANs                     : Not configured
  Open authentication            : Disabled
  MAC-move VLAN check bypass     : Disabled
```

Verify that port GigabitEthernet 1/0/1 allows multiple MAC authentication users to be authenticated.

```
[Device] display mac-authentication interface gigabitethernet 1/0/1
Global MAC authentication parameters:
  MAC authentication                  : Enabled
  Authentication method               : PAP
  Username format                     : Fixed account
          Username                    : aaa
          Password                    : ******
  MAC range accounts                  :0
          MAC address          Mask                Username
  Offline detect period               : 300 s
  Quiet period                        : 60 s
  Server timeout                      : 100 s
  Reauth period                       : 3600 s
  User aging period for critical VLAN : 1000 s
  User aging period for critical VSI  : 1000 s
  User aging period for guest VLAN    : 1000 s
  User aging period for guest VSI     : 1000 s
  Authentication domain               : sun
  HTTP proxy port list                 : Not configured
  HTTPS proxy port list                : Not configured
Online MAC-auth wired user            : 3

Silent MAC users:
```

```
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication               : Enabled
   Carry User-IP                    : Disabled
   Authentication domain            : Not configured
   Auth-delay timer                 : Disabled
   Periodic reauth                  : Disabled
   Re-auth server-unreachable       : Logoff
   Guest VLAN                       : Not configured
   Guest VLAN auth-period           : 30
   Critical VLAN                    : Not configured
   Critical voice VLAN              : Disabled
   Host mode                        : Single VLAN
   Offline detection                : Enabled
   Authentication order             : Default
   User aging                       : Enabled
   Server-recovery online-user-sync : Enabled

   Guest VSI                        : Not configured
   Guest VSI auth-period            : 30 s
   Critical VSI                     : Not configured
   Auto-tag feature                 : Disabled
   VLAN tag configuration ignoring  : Disabled
   Max online users                 : 4294967295
   Authentication attempts          : successful 0, failed 0
   Current online users             : 3
          MAC address       Auth state
          1234-0300-0011   authenticated
          1234-0300-0012   authenticated
          1234-0300-0013   authenticated
```

Verify that GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.

```
[Device] display dot1x interface gigabitethernet 1/0/1
Global 802.1X parameters:
   802.1X authentication               : Enabled
   CHAP authentication                 : Enabled
   Max-tx period                       : 30 s
   Handshake period                    : 15 s
   Offline detect period               : 300 s
   Quiet timer                         : Disabled
       Quiet period                    : 60 s
   Supp timeout                        : 30 s
   Server timeout                      : 100 s
   Reauth period                       : 3600 s
   Max auth requests                   : 2
   User aging period for Auth-Fail VLAN : 1000 s
   User aging period for Auth-Fail VSI  : 1000 s
   User aging period for critical VLAN  : 1000 s
```

```
  User aging period for critical VSI   : 1000 s
  User aging period for guest VLAN     : 1000 s
  User aging period for guest VSI      : 1000 s
  EAD assistant function               : Disabled
      EAD timeout                      : 30 min
  Domain delimiter                     : @
Online 802.1X wired users              : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Offline detection                : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : MAC-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : Not configured
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  Guest VSI                        : Not configured
  Auth-Fail VSI                    : Not configured
  Critical VSI                     : Not configured
  Add Guest VSI delay              : Disabled
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled
  Auth-Fail EAPOL                  : Disabled
  Critical EAPOL                   : Disabled

  EAPOL packets: Tx 0, Rx 0
  Sent EAP Request/Identity packets : 0
       EAP Request/Challenge packets: 0
       EAP Success packets: 0
       EAP Failure packets: 0
  Received EAPOL Start packets : 0
           EAPOL LogOff packets: 0
```

```
            EAP Response/Identity packets : 0
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 1
```

Verify that frames with an unknown destination MAC address, multicast address, or broadcast address are discarded. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 mac-authentication domain sun
 mac-authentication user-name-format fixed account aaa password cipher $c$3$HAlQ
nyXOwZXTgiOBPd7+kSPClKm7JbZ1Rw==
#
 port-security enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port-security ntk-mode ntkonly
 port-security max-mac-count 64
 port-security port-mode mac-else-userlogin-secure
#
radius scheme radsun
 primary authentication 192.168.0.38
 primary accounting 192.168.0.38
 key authentication cipher $c$3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
 key accounting cipher $c$3$UaUPGk8AfZAQLHFlbKNcEoM2HXGiuWowBQ==
 retry 5
 timer response-timeout 5
 timer realtime-accounting 15
 user-name-format without-domain
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access radius-scheme radsun
#
domain default enable sun
#
```

Example: Configuring port security to support redirect URL assignment by a ClearPass RADIUS server

Network configuration

As shown in Figure 11:

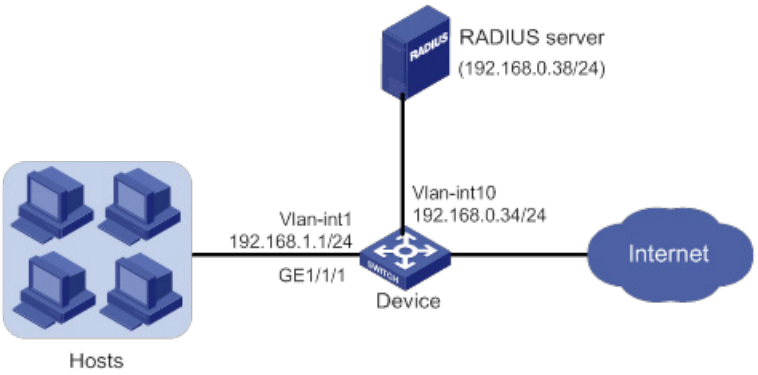
- Users on hosts are attached to port GigabitEthernet 1/0/1 on the device. All MAC authentication users use a shared user account with username **dot1x** and password **Abc123!**.
- The device acts as the NAS and a ClearPass RADIUS server performs remote authentication, authorization, and accounting for all users in domain **sun**. If a user passes authentication, the ClearPass server assigns a redirect URL to that user for Web authentication.

Configure port security mode **macAddressElseUserLoginSecureExt** on port GigabitEthernet 1/0/1 to meet the following requirements:

- Allow multiple 802.1X users and MAC authentication users to pass authentication.
- MAC authentication has a higher priority than 802.1X authentication. For an 802.1X user, the device initiates MAC authentication first, and then 802.1X authentication if the user fails MAC authentication. For a MAC authentication user, the device initiates only MAC authentication.

Set the NTK mode to **ntkonly** mode on GigabitEthernet 1/0/1 to prevent outbound frames from being sent to unknown MAC addresses.

Figure 11 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and	Release 63xx

Hardware	Software version
S5120V3-54P-PWR-SI switches)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Prerequisites

Install ClearPass Policy Manager on an ESX/ESXi Virtual Machine and set up the ClearPass server, including: importing CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf, adding resources to VMs, configuring the ClearPass management IP address (192.168.0.38 in this example), and setting the system time zone.

For more information about ClearPass server configuration, see the manual for the server.

Procedures

Configuring the ClearPass RADIUS server

The ClearPass server in this example runs CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf.

1. Log in to the ClearPass Policy Manager (CPPM).
2. On the **Configuration** > **Network** > **Devices** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
   a. Specify the IP address of the network access device (192.168.0.34 in this example).
   b. Enter the RADIUS shared secret (also referred to as RADIUS shared key). In this example, the shared secret is **expert**.
   c. Select the device vendor name.
   d. Enable RADIUS CoA and use the default port number (3799) of RADIUS CoA.
   e. Click **Add**.
3. On the **Configuration** > **Network** > **Device Groups** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
   a. Set the group name to **Group1**.
   b. Add the IP address of the network access device (192.168.0.34 in this example) to the device group.
   c. Click **Save**.
4. On the **Configuration** > **Identity** > **Local Users** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
   a. Set the user ID and name to **dot1x** and set the password to **Abc123!**,
   b. Enable the user.
   c. Select **Employee** as the user role.
   d. Click **Add**.
5. On the **Configuration** > **Identity** > **Role Mappings** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
   a. Set the role mapping policy name to **dot1x-redirect-role-map**.
   b. Select **Employee** as the default user role.
   c. On the **Mapping Rules** tab, click **Add Rule**. On the page that opens, configure the parameters as follows:
      - Select **Radius:IETF** as the type.
      - Select **User-Name** as the name.
      - Select **EQUALS** as the operator.
      - Set the value to **dot1x**.
   d. Click **Save**.
   e. On the **Summary** tab, verify that the configuration is correct.
6. On the **Configuration** > **Enforcement** > **Profiles** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:
   a. On the **Profile** tab, set the enforcement profile name to **dot1x** and select the device group that contains the network access device.
   b. On the **Attributes** tab, configure the redirect URL and specify an ACL to permit traffic that requires URL redirection. You must configure ACL rules on the network access device for the ACL.

In this example, the redirect URL is the address of the ClearPass server. The following shows the values for the redirect URL and ACL in the enforcement profile on the server:

- url-redirect=https://192.168.0.38/guest/ciscowiredguest.php?mac=%{Connection:Client-Mac-Address-Colon}
- url-redirect-acl=3001

c. Click **Save**.

d. On the **Summary** tab, verify that the configuration is correct.

7. On the **Configuration** > **Enforcement** > **Enforcement Policies** page, click **Add** at the top-right corner. On the page that opens, perform the following tasks:

a. On the **Enforcement** tab, set the enforcement policy name to **dot1x-redirect**, and select **dot1x** as the default profile. The enforcement type is RADIUS.

b. On the **Rules** tab, click **Add Rule**. On the page that opens, configure the parameters as follows.

- Set the type to **Tips**.
- Set the name to **Role**.
- Set the operator to **EQUALS**.
- Set the value to **Employee**.
- Select **[RADIUS] dot1x** as the enforcement profile.

c. Click **Save**.

d. On the **Summary** tab, verify that the configuration is correct.

8. On the **Configuration** > **Services** page, click **Add** at the top-right corner. On the page that opens, set the service name to **dot1x-wired-service**. Associate the service with other configuration items in different tabs and save the configuration.

- Select PAP as the authentication method.
- Add authentication source **[Guest User Repository] [Local SQL DB]**.
- Select **dot1x-redirect-role-map** as the role mapping policy.
- Select **dot1x-redirect** as the enforcement policy.

9. On the **Summary** page, verify that the configuration is correct.

Configuring the device

1. Assign an IP address to each interface, as shown in Figure 11. Make sure the hosts, device, and RADIUS server can reach each other. (Details not shown.)

2. Configure the RADIUS scheme:

Create RADIUS scheme **radsun**.

```
<Device> system-view
[Device] radius scheme radsun
New RADIUS scheme.
```

Specify the server at 192.168.0.38 as the primary RADIUS authentication server.

```
[Device-radius-radsun] primary authentication 192.168.0.38
```

Specify the server at 192.168.0.38 as the primary RADIUS accounting server.

```
[Device-radius-radsun] primary accounting 192.168.0.38
```

Set the authentication shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key authentication simple expert
```

Set the accounting shared key to **expert** in plain text for secure communication between the device and the RADIUS server.

```
[Device-radius-radsun] key accounting simple expert
```

Exclude domain names from the usernames sent to the RADIUS server.

```
[Device-radius-radsun] user-name-format without-domain
```

Specify 192.168.0.34 as the source IP address of outgoing RADIUS packets.

```
[Device-radius-radsun] nas-ip 192.168.0.34
[Device-radius-radsun] quit
```

Create ISP domain **sun** and enter ISP domain view.

```
[Device] domain sun
```

Configure ISP domain **sun** to use RADIUS scheme **radsun** for authentication, authorization, and accounting of all LAN users.

```
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

Specify ISP domain **sun** as the default domain.

```
[Device] domain default enable sun
```

3. Configure port security:

Enable port security globally.

```
[Device] port-security enable
```

Set the port security mode to **macAddressElseUserLoginSecureExt** and set the NTK mode to **ntkonly** on GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode
mac-else-userlogin-secure-ext
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Device-GigabitEthernet1/0/1] quit
```

Configure a shared account for MAC authentication users, and set the username to **dot1x** and password to plaintext string of **Abc123!**.

```
[Device] mac-authentication user-name-format fixed account dot1x password simple
Abc123!
```

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
[Device] dot1x authentication-method pap
```

4. Configure advanced ACL 3001 to permit traffic destined for the redirect URL. The redirect URL is the address of the ClearPass server. Make sure the ACL number is the same as that assigned by the ClearPass server.

```
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule 0 permit ip destination 192.168.0.38 0
[Device-acl-ipv4-adv-3001] quit
```

Verifying the configuration

Verify that port security is correctly configured.

```
[Device] display port-security interface gigabitethernet 1/0/1
Global port security parameters:
   Port security          : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
```

```
  Blockmac timeout       : 180 s
  MAC move               : Denied
  Authorization fail     : Online
  NAS-ID profile         : Not configured
  Dot1x-failure trap     : Disabled
  Dot1x-logon trap       : Disabled
  Dot1x-logoff trap      : Disabled
  Intrusion trap         : Disabled
  Address-learned trap   : Disabled
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
  Open authentication    : Disabled
  Traffic-statistics     : Disabled
  OUI value list         :

 GigabitEthernet1/0/1 is link-up
  Port mode                      : macAddressElseUserloginSecureExt
  NeedToKnow mode                : NeedToKnowOnly
  Intrusion protection mode      : NoAction
  Security MAC address attribute
      Learning mode              : Sticky
      Aging type                 : Periodical
  Max secure MAC addresses       : Not configured
  Current secure MAC addresses   : 0
  Authorization                  : Permitted
  NAS-ID profile                 : Not configured
  Free VLANs                     : Not configured
  Open authentication            : Disabled
  MAC-move VLAN check bypass     : Disabled
```

Display MAC authentication information on GigabitEthernet 1/0/1.

```
[Device] display mac-authentication interface gigabitethernet 1/0/1
Global MAC authentication parameters:
  MAC authentication                  : Enabled
  Authentication method               : PAP
  Username format                     : Fixed account
          Username                    : dot1x
          Password                    : ******
  MAC range accounts                  :0
          MAC address          Mask                Username
  Offline detect period               : 300 s
  Quiet period                        : 60 s
  Server timeout                      : 100 s
  Reauth period                       : 3600 s
  User aging period for critical VLAN : 1000 s
  User aging period for critical VSI  : 1000 s
  User aging period for guest VLAN    : 1000 s
  User aging period for guest VSI     : 1000 s
```

```
  Authentication domain              : sun
  HTTP proxy port list                : Not configured
  HTTPS proxy port list               : Not configured
 Online MAC-auth wired user           : 1

 Silent MAC users:
         MAC address       VLAN ID  From port              Port index

 GigabitEthernet1/0/1  is link-up
  MAC authentication               : Enabled
  Carry User-IP                    : Disabled
  Authentication domain            : sun
  Auth-delay timer                 : Disabled
  Periodic reauth                  : Disabled
  Re-auth server-unreachable       : Logoff
  Guest VLAN                       : Not configured
  Guest VLAN auth-period           : 30 s
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Host mode                        : Single VLAN
  Offline detection                : Enabled
  Authentication order             : Default
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled

  Guest VSI                        : Not configured
  Guest VSI auth-period            : 30 s
  Critical VSI                     : Not configured
  Auto-tag feature                 : Disabled
  VLAN tag configuration ignoring  : Disabled
  Max online users                 : 4294967295
  Authentication attempts          : successful 5, failed 38
  Current online users             : 1
         MAC address       Auth state
         acf1-df6c-ff48    Authenticated
```

Display 802.1X information on GigabitEthernet 1/0/1.

```
[Device] display dot1x interface gigabitethernet 1/0/1
Global 802.1X parameters:
  802.1X authentication              : Enabled
  PAP authentication                 : Enabled
  Max-tx period                      : 30 s
  Handshake period                   : 15 s
  Offline detect period              : 300 s
  Quiet timer                        : Disabled
      Quiet period                   : 60 s
  Supp timeout                       : 30 s
  Server timeout                     : 100 s
  Reauth period                      : 3600 s
```

```
  Max auth requests                   : 2
  User aging period for Auth-Fail VLAN : 1000 s
  User aging period for Auth-Fail VSI  : 1000 s
  User aging period for critical VLAN  : 1000 s
  User aging period for critical VSI   : 1000 s
  User aging period for guest VLAN     : 1000 s
  User aging period for guest VSI      : 1000 s
  EAD assistant function               : Disabled
      EAD timeout                      : 30 min
  Domain delimiter                     : @
Online 802.1X wired users              : 0

GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Offline detection                : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : MAC-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : Not configured
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  Guest VSI                        : Not configured
  Auth-Fail VSI                    : Not configured
  Critical VSI                     : Not configured
  Add Guest VSI delay              : Disabled
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled
  Auth-Fail EAPOL                  : Disabled
  Critical EAPOL                   : Disabled

  EAPOL packets: Tx 165, Rx 0
  Sent EAP Request/Identity packets : 165
       EAP Request/Challenge packets: 0
```

```
        EAP Success packets: 0
        EAP Failure packets: 0
   Received EAPOL Start packets : 0
            EAPOL LogOff packets: 0
            EAP Response/Identity packets : 0
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 0
```

Display online user information after users pass authentication.

```
<Device> display mac-authentication connection
Total connections: 1
Slot ID: 2
User MAC address: acf1-df6c-ff48
Access interface: GigabitEthernet1/0/1
Username: dot1x
User access state: Successful
Authentication domain: sun
IPv4 address: 192.168.1.5
Initial VLAN: 4
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL:
https://192.168.0.38/guest/ciscowiredguest.php?mac=ac:f1:df:6c:ff:48
Termination action: Default
Session timeout period: N/A
Online from: 2018/03/02 12:52:17
Online duration: 0h 11m 12s
```

Verify that frames with an unknown destination MAC address, multicast address, or broadcast address are discarded on GigabitEthernet 1/0/1. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 dot1x authentication-method pap
#
 mac-authentication user-name-format fixed account dot1x password cipher $c$3$HAlQ
nyXOwZXTgiOBPd7+kSPClKm7JbZ1Rw==
#
 port-security enable
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port-security ntk-mode ntkonly
 port-security port-mode mac-else-userlogin-secure-ext
#
acl advanced 3001
 rule 0 permit ip destination 192.168.0.38 0
#
radius scheme radsun
 primary authentication 192.168.0.38
 primary accounting 192.168.0.38
 key authentication cipher $c$3$s9TAYm34R8sS5k/Cylg2sDm69ZRupMvGJg==
 key accounting cipher $c$3$UaUPGk8AfZAQLHFlbKNcEoM2HXGiuWowBQ==
 retry 5
 user-name-format without-domain
 nas-ip 192.168.0.34
#
domain sun
 authentication lan-access radius-scheme radsun
 authorization lan-access radius-scheme radsun
 accounting lan-access radius-scheme radsun
#
domain default enable sun
#
```

Contents

Introduction

This document provides examples for configuring the following portal authentications:

- **Cross-subnet authentication**—Applies to networks where Layer 3 forwarding devices exist between the authentication client and the access device. After a user passes authentication on an interface, the access device generates an ACL for the user based on the user's IP address to permit packets from the user on the interface.
- **Direct authentication**—Applies to networks where no layer 3 forwarding devices exist between the authentication client and the access device. In such a network, the access device can learn MAC addresses of users. The access device can use both ACLs and MAC addresses to enhance control on user packet forwarding.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of portal.

Restrictions and guidelines

When you configure direct or cross-subnet portal authentication, follow these restrictions and guidelines:

- Only the RADIUS server can perform authentication, authorization, and accounting for portal users.
- On the RADIUS server, configure routes to reach the authentication interfaces and user networks.
- The IMC server uses session control packets to send disconnection requests to the access device. If you use the IMC server as the RADIUS server, execute the **`radius session-control enable`** command on the access device. Otherwise, the access device cannot receive portal user logout requests from the RADIUS server.
- When the access device runs Portal 2.0, configure the BAS-IP attribute for portal packets sent to the portal authentication server. Make sure the BAS-IP is the same as the **IP Address** configured on the portal authentication server. Otherwise, the portal authentication server will drop unsolicited portal packets (such as logout notifications) from the access device.

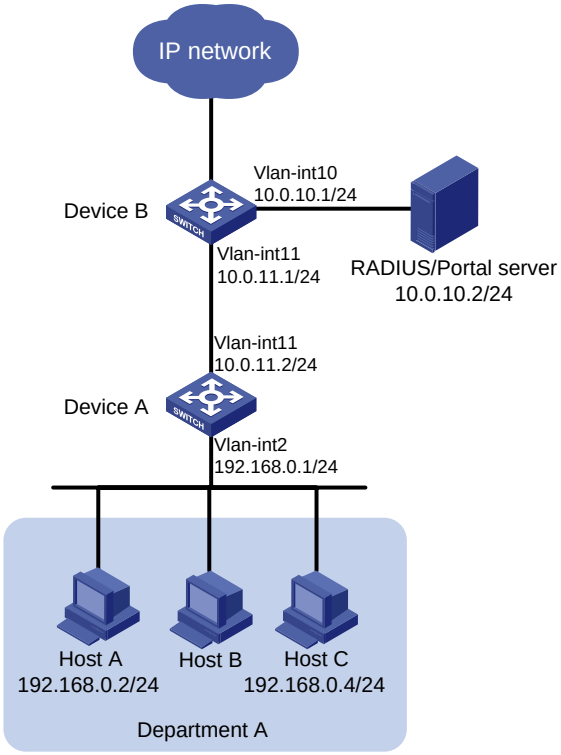
Example: Configuring cross-subnet portal authentication

Network configuration

As shown in Figure 1, Device B supports portal authentication. An IMC server acts as a portal authentication server, a portal Web server, and a RADIUS server. The RADIUS server is used to perform AAA on portal users. In this example, the IMC server runs IMC PLAT 7.0 (E0202) and IMC UAM 7.0 (E0202).

Configure cross-subnet portal authentication. Before passing authentication, a host can access only the portal server. After passing authentication, the host can access resources in the IP network.

Figure 1 Network diagram



Analysis

To enable Device B to perform cross-subnet portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable cross-subnet portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

Hardware	Software version
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx

Hardware	Software version
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Configuring Device A

Configure VLAN-interface 2 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 11
[DeviceA-vlan11] quit
```

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 11
[DeviceA-Vlan-interface11] ip address 10.0.11.2 24
[DeviceA-Vlan-interface11] quit
```

Assign the corresponding physical interfaces to the VLANs. (Details not shown.)

Configure a static route to the RADIUS server.

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

Configuring Device B

Configure VLAN-interface 10 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] interface vlan-interface 11
[DeviceB-Vlan-interface11] ip address 10.0.11.1 24
[DeviceB-Vlan-interface11] quit
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] ip address 10.0.10.1 24
[DeviceB-Vlan-interface10] quit
```

Configure portal authentication server **newpt**.

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

Enable cross-subnet authentication on VLAN-interface 11, the interface connected to Device A.

```
[DeviceB] interface Vlan-interface 11
[DeviceB-Vlan-interface11] portal enable method layer3
```

Configure the BAS-IP as 10.0.11.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.

```
[DeviceB-Vlan-interface11] portal bas-ip 10.0.11.1
```

Specify portal Web server **newpt** on VLAN-interface 11.

```
[DeviceB-Vlan-interface11] portal apply web-server newpt
[DeviceB-Vlan-interface11] quit
```

Create a RADIUS scheme named **imc** and enter its view.

```
[DeviceB] radius scheme imc
```

Specify the primary authentication and accounting server, and configure the keys for communication with the server.

```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
```

Enable the RADIUS session-control feature.

```
[DeviceB] radius session-control enable
```

Create an ISP domain named **portal.com** and enter its view.

```
[DeviceB] domain portal.com
```

Configure AAA methods for the ISP domain.

```
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
```

Specify domain **portal.com** as the default ISP domain. If a user enters the username without the ISP domain name at login, the AAA methods of the default domain are used for the user.

```
[DeviceB] domain default enable portal.com
```

Configure a static route to Department A.

```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

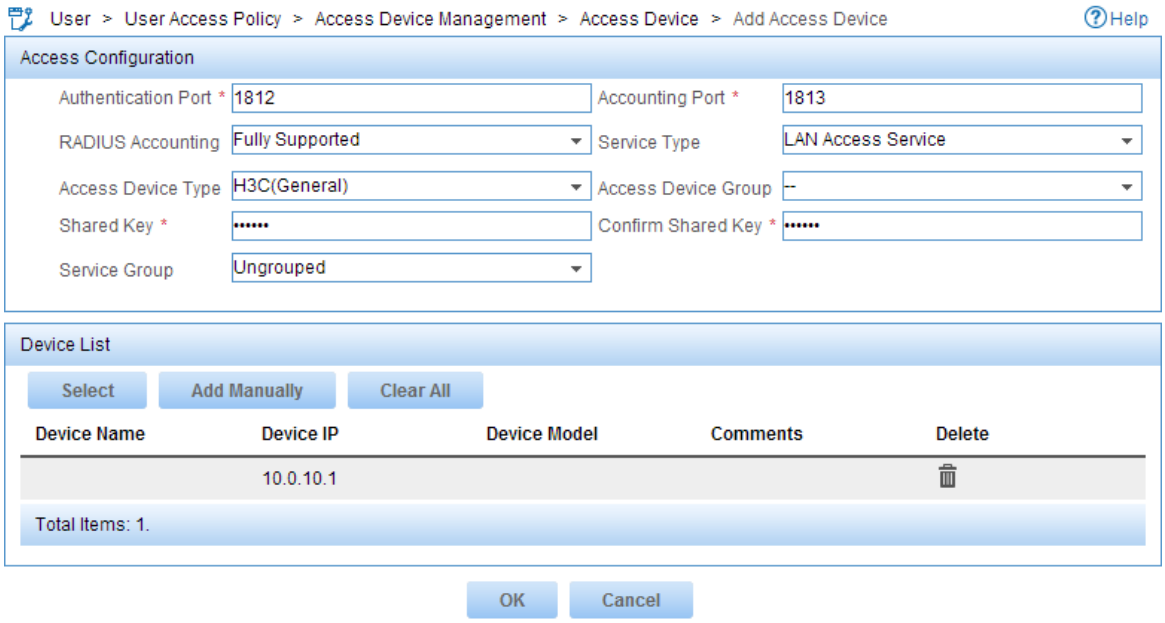
Configuring the RADIUS and portal server

Adding an access device

1. Log in to IMC, and click the **User** tab.
2. From the navigation tree, select **User Access Manager** > **Access Device Management** > **Access Device**.
3. Click **Add**.

   The **Add Access Device** page appears.
4. In the **Access Configuration** area, configure the following parameters:
   - Enter **expert** in the **Shared Key** and **Confirm Shared Key** fields.
   - Enter **1812** in the **Authentication Port** field and **1813** in the **Accounting Port** field.
   - Select **LAN Access Service** from the **Service Type** list.
   - Select **H3C(General)** from the **Access Device Type** list.
5. In the **Device List** area, click **Add Manually**.
6. On the page that appears, enter IP address **10.0.10.1** in the **Start IP** field, and click **OK**.
7. Click **OK**.

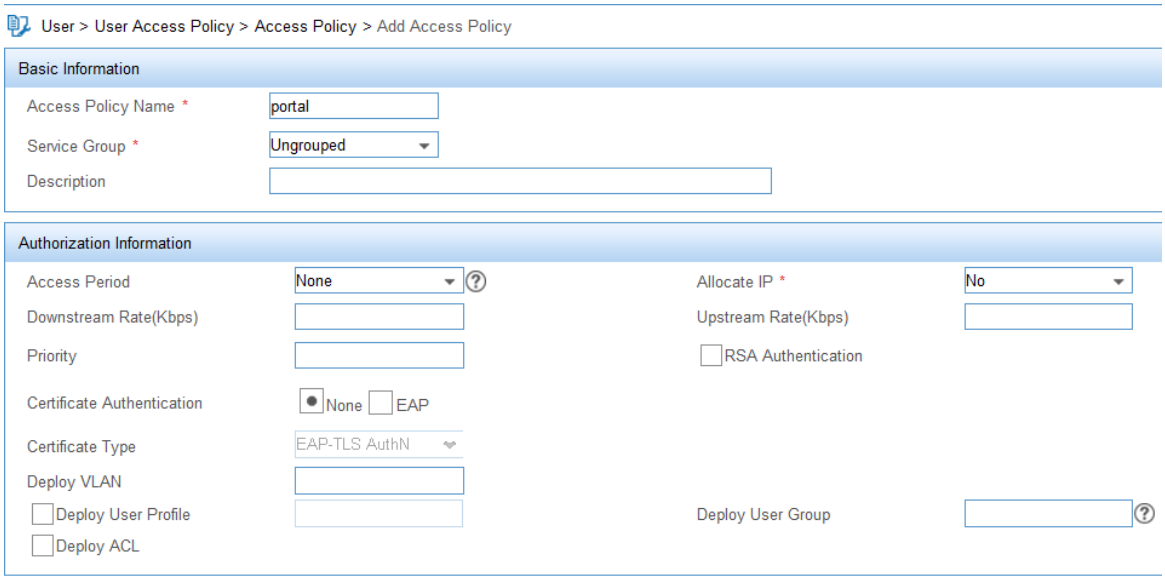
Figure 2 Adding an access device



Adding an access policy

1. Click the **User** tab.
2. From the navigation tree, select **User Access Manager** > **Access Policy**.
3. Click **Add**.
4. On the page that appears, enter **portal** in the **Access Policy Name** field. Use the default settings for other parameters.
5. Click **OK**.

Figure 3 Adding an access policy

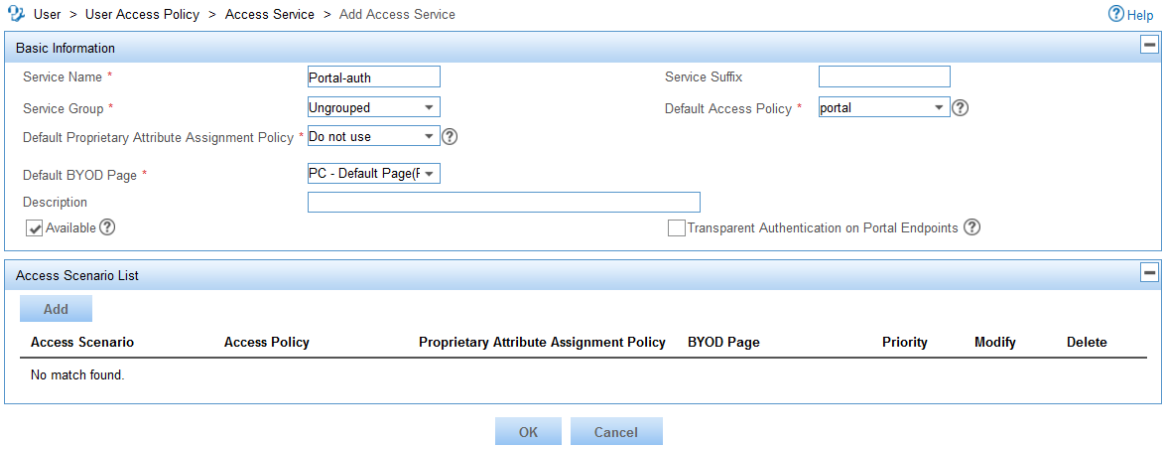


Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Manager** > **Access Service**.

3. Click **Add**.
4. On the page that appears, configure the following parameters:
   - Enter **Portal-auth** in the **Service Name** field.
   - Select **portal** from the **Default Access Policy** list.
   - Use the default settings for other parameters.
5. Click **OK**.

Figure 4 Adding an access service

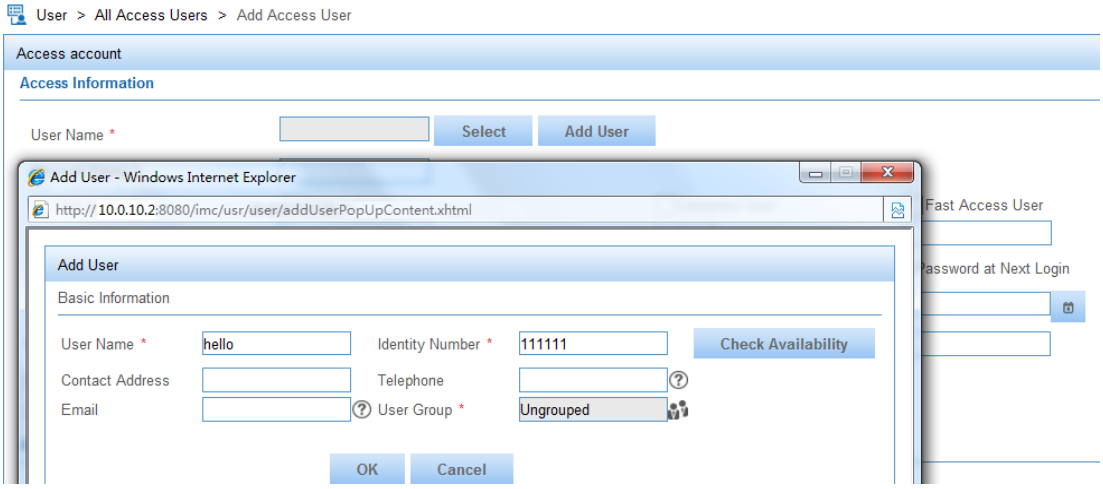


Configuring an access user

1. Click the **User** tab.
2. From the navigation tree, select **Access User**> **All Access Users**.
3. Click **Add**.

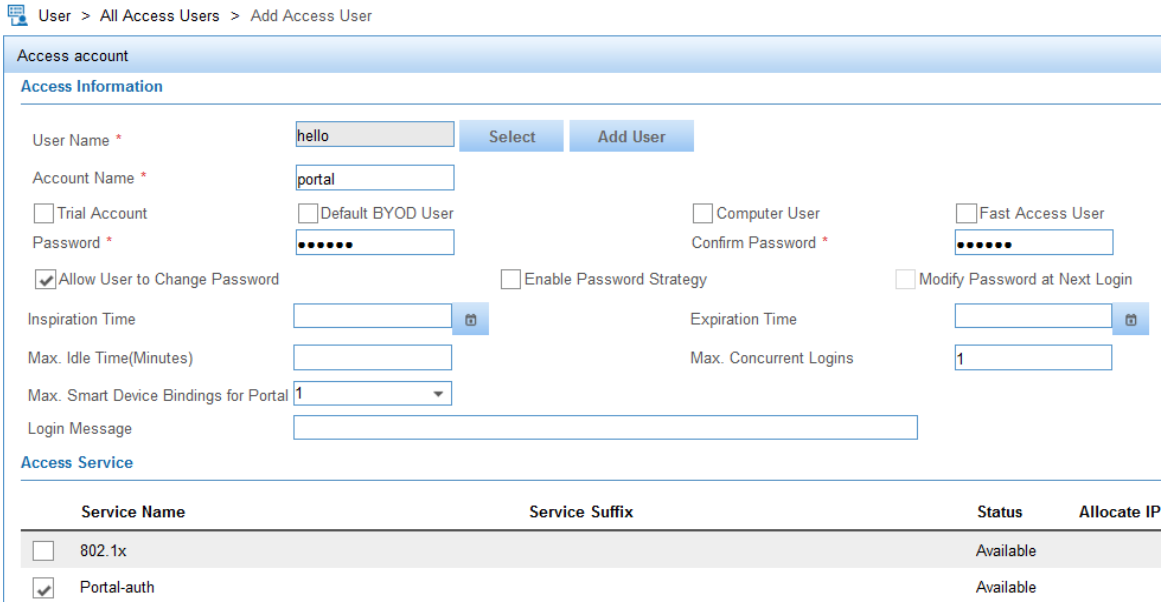
   The **Add Access User** page appears.
4. In the **Access Information** area, click the **Add User** button for the **User Name** field.
5. On the page that appears, configure the following parameters:
   - Enter **hello** in the **User Name** field.
   - Enter **111111** in the **Identity Number** field.
   - Use the default settings for other parameters.
   - Click **OK**.

Figure 5 Adding a user



6. In the **Access Information** area, enter **portal** in the **Account Name** field and configure the password as **123456** for the account.
7. In the **Access Service** area, select the access service named **Portal-auth**.
8. Use the default settings for other parameters.
9. Click **OK**.

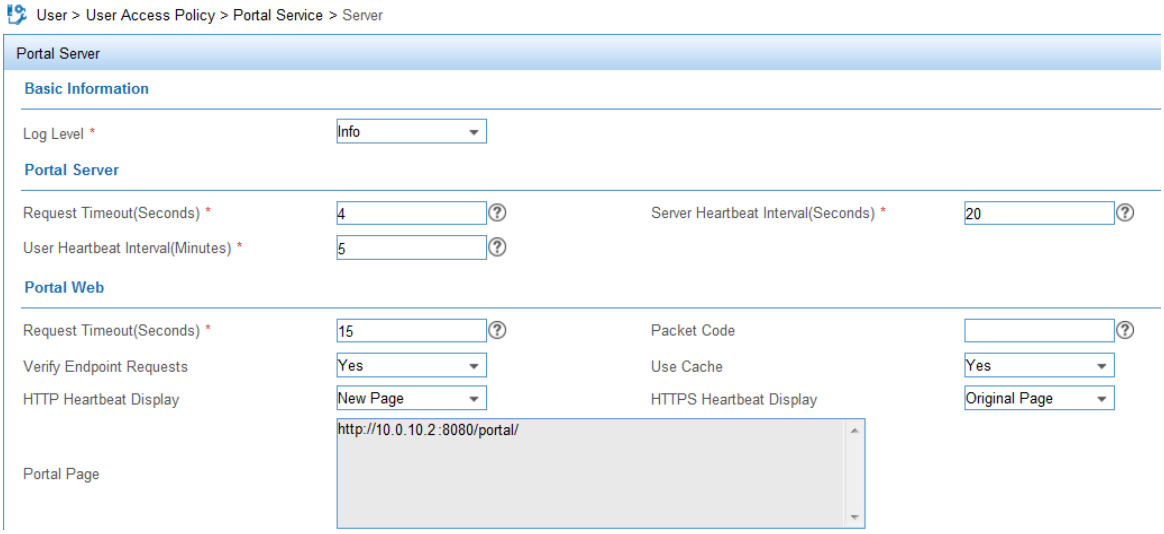
Figure 6 Configuring an access user



Configuring a portal page

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy** > **Portal Service** > **Server**.
3. Use the default settings for all parameters.
4. Click **OK**.

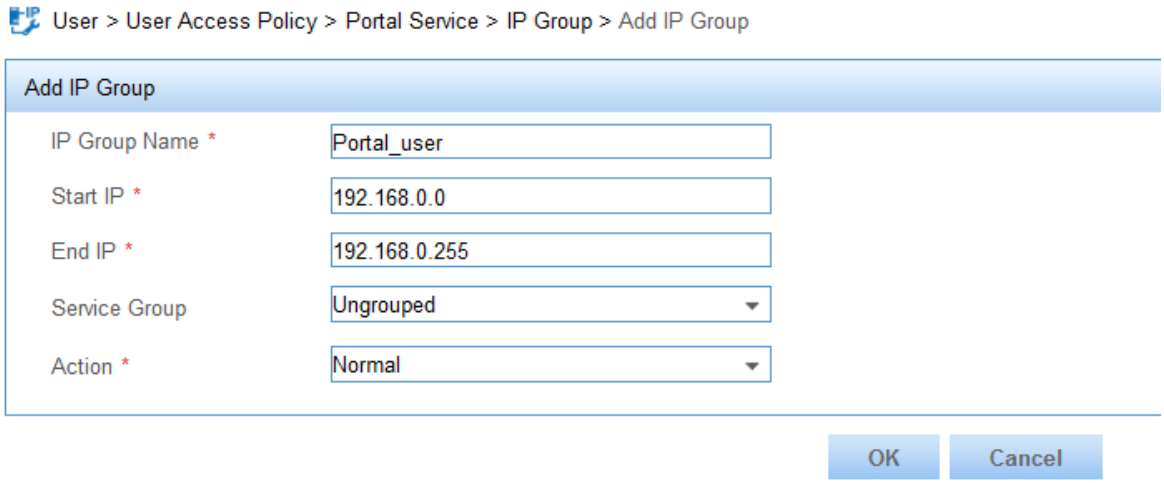
Figure 7 Configuring a portal page



Adding an IP group for portal authentication

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy** > **Portal Service** > **IP Group**.
3. Click **Add**.
4. On the page that appears, configure the following parameters:
   - Enter **Portal_user** in the **IP Group Name** field.
   - Enter **192.168.0.0** in the **Start IP** field and **192.168.0.255** in the **End IP** field.
   - Use the default settings for other parameters.
5. Click **OK**.

Figure 8 Adding an IP group

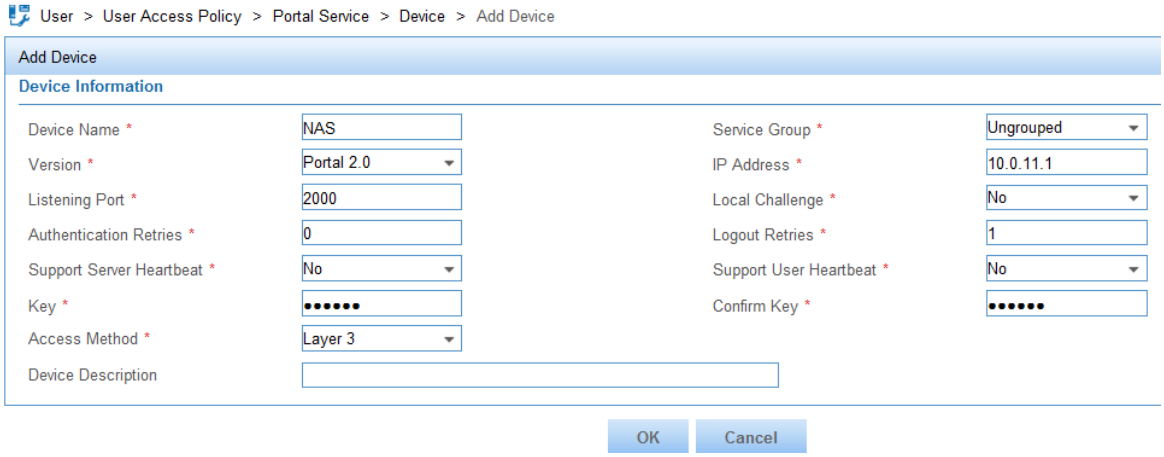


Configuring an access device for portal authentication

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy** > **Portal Service** > **Device**.
3. Click **Add**.
4. On the **Add Device** page, configure the following parameters:
   - Enter **NAS** in the **Device Name** field.
   - Enter **10.0.11.1** in the **IP Address** field.
   - Enter **portal** in the **Key** and **Confirm Key** fields.

     The key must be the same as that for the portal authentication server configured on Device B.
   - Select **Layer 3** from the **Access Method** list.
   - Use the default settings for other parameters.
5. Click **OK**.

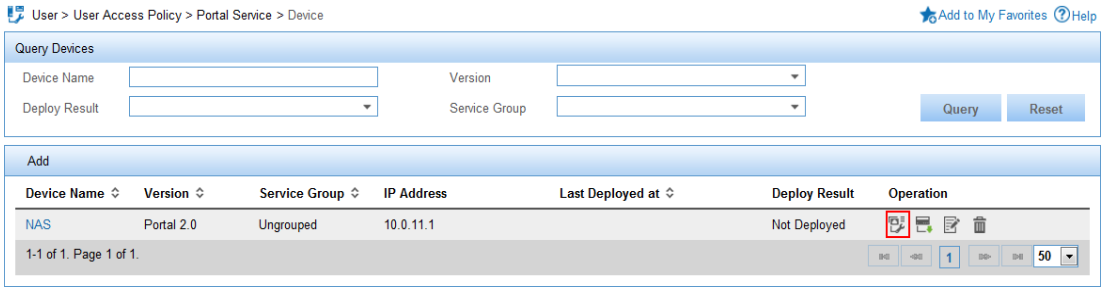
Figure 9 Adding an access device



Configuring a port group for portal authentication

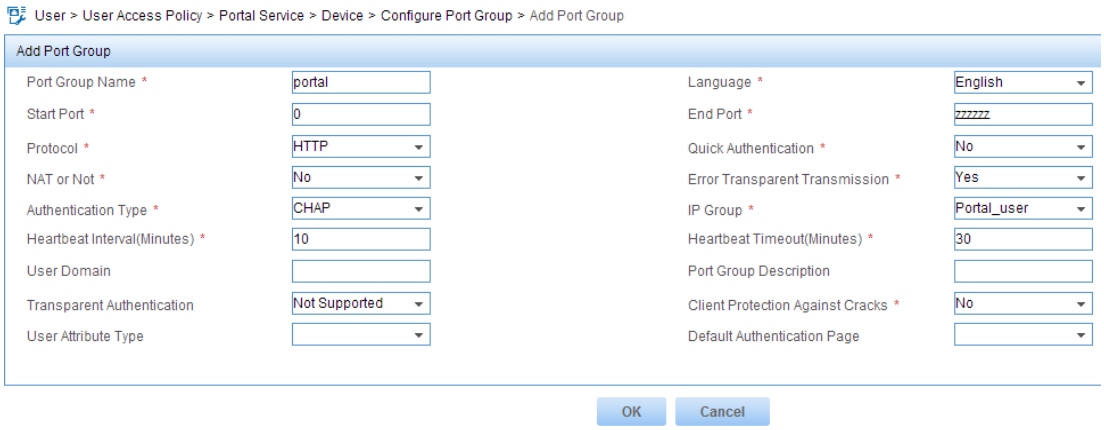
1. On the **Device** page, click the **Port Group** icon.

   Figure 10 Accessing the Device page



2. On the **Configure Port Group** page, click **Add**.
3. On the **Add Port Group** page, configure the following parameters:
   - Enter **portal** in the **Port Group Name** field.
   - Select **Portal_user** from the **IP Group** list.
   - Use the default settings for other parameters.
4. Click **OK**.

   Figure 11 Adding a port group



Verifying the configuration

A user can perform portal authentication by using the H3C iNode client or through a Web page. This example triggers portal authentication by accessing a Web page.

Access a Web page through a Web browser on a host. You are redirected to the authentication page **http://10.0.10.2:8080/portal**. Enter the username **portal** and the password **123456** to log in. After passing the authentication, you are redirected to the authentication success page.

Execute the **display portal user** command on Device B to display the portal user information.

```
[DeviceB] display portal user interface vlan-interface 11
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC              IP               Vlan   Interface
  0015-e9a6-7cfe   192.168.0.2      11     Vlan-interface11
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Configuration files

- Device A:

```
#
vlan 2
#
vlan 11
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
#
```

- Device B:

```
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
```

```
#
interface Vlan-interface11
 ip address 10.0.11.1 255.255.255.0
 portal enable method layer3
 portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
ip route-static 192.168.0.0 24 10.0.11.2
#
radius session-control enable
#
radius scheme imc
primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

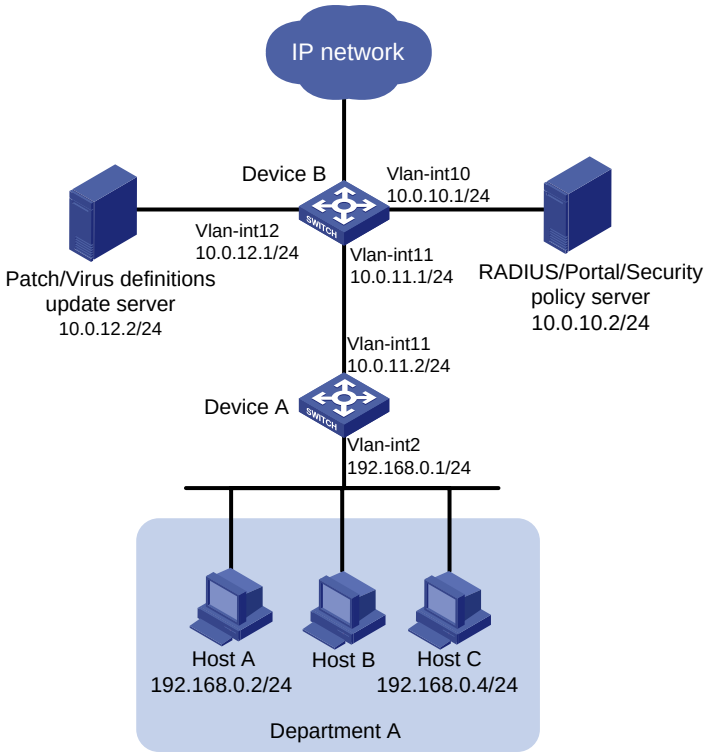
Example: Configuring extended cross-subnet portal authentication

Network configuration

As shown in Figure 12, Device B supports portal authentication. An IMC server acts as a portal authentication server, a portal Web server, a RADIUS server, and a security policy server. The RADIUS server is used to perform AAA on portal users. The security policy server is deployed to perform security check on portal-authenticated users. In this example, the IMC server runs IMC PLAT 7.0 (E0202) and IMC UAM 7.0 (E0202).

Configure extended cross-subnet portal authentication. Before passing portal authentication, a host can access only the portal Web server. After the host passes authentication, the security policy server performs a security check on the host. If the host fails the security check, the host is permitted to access only the Patch/Virus definitions update server. After passing the security check, the host can access resources in the IP network.

Figure 12 Network diagram



Analysis

To enable Device B to perform cross-subnet portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable cross-subnet portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

To perform security check on authenticated users, you must complete the following tasks:

- On Device B, create an ACL (ACL 3000 in this example) for users who fail security checks, and an ACL (ACL 3001 in this example) for users who pass security checks.
- On the security policy server, specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-	Release 63xx

Hardware	Software version
54P-PWR-SI switches)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Configuring Device A

Configure VLAN-interface 2 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 11
```

```
[DeviceA-vlan11] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 11
[DeviceA-Vlan-interface11] ip address 10.0.11.2 24
[DeviceA-Vlan-interface11] quit
```

Assign the corresponding physical interfaces to the VLANs. (Details not shown.)

Configure a static route to the RADIUS, portal, and security policy server.

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

Configure a static route to the patch and virus definitions update server.

```
[DeviceA] ip route-static 10.0.12.0 255.255.255.0 10.0.11.1
```

Configuring Device B

Configure VLAN-interface 10, VLAN-interface 11, and VLAN-interface 12, and assign them IP addresses.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 12
[DeviceB-vlan12] quit
[DeviceB] interface vlan-interface 11
[DeviceB-Vlan-interface11] ip address 10.0.11.1 24
[DeviceB-Vlan-interface11] quit
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] ip address 10.0.10.1 24
[DeviceB-Vlan-interface10] quit
[DeviceB] interface vlan-interface 12
[DeviceB-Vlan-interface12] ip address 10.0.12.1 24
[DeviceB-Vlan-interface12] quit
```

Configure the portal authentication server **newpt**.

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

Enable cross-subnet authentication on VLAN-interface 11, the interface connected to Device A.

```
[DeviceB] interface Vlan-interface 11
[DeviceB-Vlan-interface11] portal enable method layer3
```

Configure the BAS-IP as 10.0.11.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.

```
[DeviceB-Vlan-interface11] portal bas-ip 10.0.11.1
```

Specify portal Web server **newpt** on VLAN-interface 11.

```
[DeviceB-Vlan-interface11] portal apply web-server newpt
[DeviceB-Vlan-interface11] quit
```

Create a static route to Department A.

```
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

Create RADIUS scheme named **imc** and enter its view.

```
[DeviceB] radius scheme imc
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the server.

```
[DeviceB-radius-imc] primary authentication 10.0.10.2
[DeviceB-radius-imc] primary accounting 10.0.10.2
[DeviceB-radius-imc] key authentication simple expert
[DeviceB-radius-imc] key accounting simple expert
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[DeviceB-radius-imc] user-name-format without-domain
[DeviceB-radius-imc] quit
```

Enable RADIUS session control.

```
[DeviceB] radius session-control enable
```

Create an ISP domain named **portal.com** and enter its view.

```
[DeviceB] domain portal.com
```

Configure AAA methods for the ISP domain.

```
[DeviceB-isp-portal.com] authentication portal radius-scheme imc
[DeviceB-isp-portal.com] authorization portal radius-scheme imc
[DeviceB-isp-portal.com] accounting portal radius-scheme imc
[DeviceB-isp-portal.com] quit
```

Specify domain **portal.com** as the default ISP domain. If a user enters the username without the ISP domain name at login, the AAA methods of the default domain are used for the user.

```
[DeviceB] domain default enable portal.com
```

Configure ACL 3000 to permit access only to the Patch/Virus definitions update server and ACL 3001 to permit access to any IP address.

```
[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule permit ip destination 10.0.12.2 0
[DeviceB-acl-adv-3000] rule deny ip
[DeviceB-acl-adv-3000] quit
[DeviceB] acl number 3001
[DeviceB-acl-adv-3001] rule permit ip
[DeviceB-acl-adv-3001] quit
```

Configuring the RADIUS, portal, and security policy server

Configure the RADIUS server and portal server. For more information, see "Configuring the RADIUS and portal server."

Configure the security policy server. Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

Verifying the configuration

A user can perform the extended cross-subnet authentication only by using the H3C iNode client.

Open the iNode client on a host, and create a portal connection. Enter the username and password and click **Connect**. The user passes the portal authentication.

On the iNode client, check security check information. The user failed to pass the security check.

Display portal user information on Device B to verify that ACL 3000 has been deployed to the user.

```
[DeviceB] display portal user all
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                    VLAN    Interface
  0015-e9a6-7cfe  192.168.0.2            11     Vlan-interface11
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3000
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Update the virus database on the host to meet the security requirement.

On the iNode client, disconnect the portal connection and then log in again. Check security check information. The iNode client displays that the host successfully passed the security check.

Display portal user information on Device B to verify that ACL 3001 has been deployed to the portal user.

```
[DeviceB]display portal user all
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: N/A
  MAC             IP                    VLAN    Interface
  0015-e9a6-7cfe  192.168.0.2            11      Vlan-interface11
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3001
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Configuration files

- Device A:

```
#
vlan 2
#
vlan 11
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
ip route-static 10.0.12.0 24 10.0.11.1
#
```

- Device B:

```
#
vlan 10 to 12
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.1 255.255.255.0
portal enable method layer3
portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
interface Vlan-interface12
 ip address 10.0.12.1 255.255.255.0
#
ip route-static 192.168.0.0 24 10.0.11.2
#
acl number 3000
 rule 0 permit ip destination 10.0.12.2 0
 rule 5 deny ip
#
acl number 3001
 rule 0 permit ip
#
 radius session-control enable
#
radius scheme imc
 primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
```

```
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
 user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
 domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

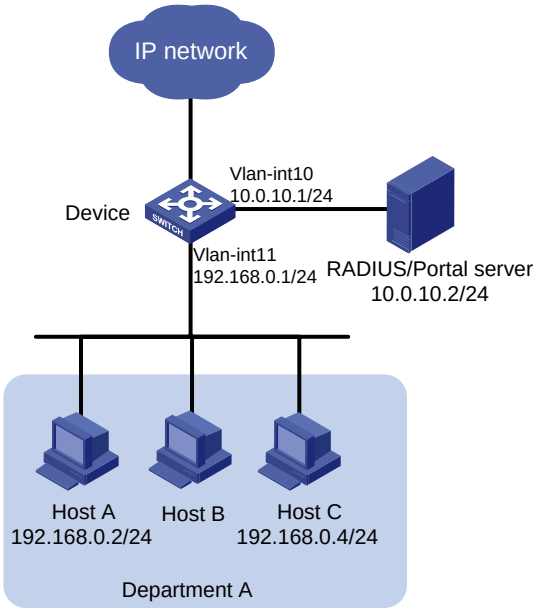
Example: Configuring direct portal authentication

Network configuration

As shown in Figure 13, hosts in Department A are directly connected to the device. An IMC server acts as a portal authentication server, a portal Web server, and a RADIUS server. The RADIUS server is used to perform AAA on portal users. In this example, the IMC server runs IMC PLAT 7.0 (E0202) and IMC UAM 7.0 (E0202).

Configure direct portal authentication. The hosts can access only the portal server before passing authentication and can access other network resources after passing authentication.

Figure 13 Network diagram



Analysis

To enable the device to perform portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable direct portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

Hardware	Software version
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

Hardware	Software version
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Configuring the device

Configure VLAN-interface 10 and VLAN-interface 11, and assign them IP addresses.

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
[Device] vlan 11
[Device-vlan11] quit
[Device] interface vlan-interface 11
[Device-Vlan-interface11] ip address 192.168.0.1 24
[Device-Vlan-interface11] quit
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 10.0.10.1 24
[Device-Vlan-interface10] quit
```

Configure the portal authentication server **newpt**.

```
[Device] portal server newpt
[Device-portal-server-newpt] ip 10.0.10.2 key simple portal
[Device-portal-server-newpt] port 50100
[Device-portal-server-newpt] quit
```

Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[Device] portal web-server newpt
[Device-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[Device-portal-websvr-newpt] quit
```

Enable direct portal authentication on VLAN-interface 11.

```
[Device] interface Vlan-interface 11
[Device-Vlan-interface11] portal enable method direct
```

Configure the BAS-IP as 192.168.0.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.

```
[Device-Vlan-interface11] portal bas-ip 192.168.0.1
```

Specify portal Web server **newpt** on VLAN-interface 11.

```
[Device-Vlan-interface11] portal apply web-server newpt
[Device-Vlan-interface11] quit
```

Create a RADIUS scheme named **imc** and enter its view.

```
[Device] radius scheme imc
```

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the server.

```
[Device-radius-imc] primary authentication 10.0.10.2
[Device-radius-imc] primary accounting 10.0.10.2
[Device-radius-imc] key authentication simple expert
[Device-radius-imc] key accounting simple expert
```

Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Device-radius-imc] user-name-format without-domain
[Device-radius-imc] quit
```

Enable the RADIUS session-control feature.

```
[Device] radius session-control enable
```

Create an ISP domain named **portal.com** and enter its view.

```
[Device] domain portal.com
```

Configure AAA methods for the ISP domain.

```
[Device-isp-portal.com] authentication portal radius-scheme imc
[Device-isp-portal.com] authorization portal radius-scheme imc
[Device-isp-portal.com] accounting portal radius-scheme imc
[Device-isp-portal.com] quit
```

Specify ISP domain **portal.com** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Device] domain default enable portal.com
```

Configuring the RADIUS and portal server

Configure the RADIUS server and portal server. For more information, see "Configuring the RADIUS and portal server."

When you configuring an access device for portal authentication (as shown in Figure 13), select **Directly Selected** from the **Access Method** list, and enter **192.168.0.1** in the **IP Address** field.

Verifying the configuration

A user can perform portal authentication by using the H3C iNode client or through a Web page. This example uses the Web page.

Access a Web page through a Web browser on a host. You are redirected to the authentication page **http://10.0.10.2:8080/portal**. Enter the username **portal** and the password **123456** to log in. After passing the authentication, you are redirected to the authentication success page.

Execute the **display portal user** command to display portal user information on Device.

```
[Device] display portal user interface vlan-interface 11
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP              Vlan   Interface
```

```
  0015-e9a6-7cfe   192.168.0.2       11     Vlan-interface11
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Configuration files

```
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
#
interface Vlan-interface11
 ip address 192.168.0.1 255.255.255.0
 portal enable method direct
 portal bas-ip 192.168.0.1
 portal apply web-server newpt
#
radius session-control enable
#
radius scheme imc
primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme imc
 authorization portal radius-scheme imc
accounting portal radius-scheme imc
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```

Contents

Introduction

This document provides SSH configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of SSH.

General restrictions and guidelines

The devices in the configuration examples operate in non-FIPS mode.

When you configure SSH on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of the key pair must be 2048 bits.
- When the device acts as an SSH server, only RSA key pairs are supported. Do not generate a DSA key pair on the SSH server.

Example: Configuring the device as an Stelnet server using password authentication

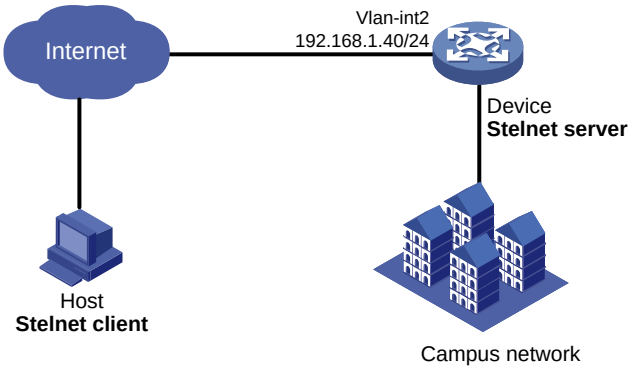
Network configuration

As shown in Figure 1:

- The device uses local password authentication.
- The login username and password are **client001** and **hello12345**, respectively.

Establish an Stelnet connection between the host and the device, so you can log in to the device to manage the campus network.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA and RSA key pairs on the server.
- To perform local authentication, create a local user and configure a password for the local user on the Stelnet server.
- To enable an SSH user to use all commands after login, set the user role of the local user to network-admin. By default, the user role of a local user is network-operator.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series	Release 63xx

Hardware	Software version
S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Generate RSA key pairs.

```
<Device> system-view
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
..
Create the key pair successfully.
```

Generate a DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
......
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the SSH server function.

```
[Device] ssh server enable
```

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The Stelnet client uses the IP address as the destination address of the Stelnet connection.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Device-Vlan-interface2] quit
```

Set the authentication mode to AAA (**scheme**) for the user lines.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Create a local user **client001**.

```
[Device] local-user client001 class manage
New local user added.
```

Set the password to **hello12345** in plain text for the local user **client001**.

```
[Device-luser-manage-client001] password simple hello12345
```

Authorize the local user **client001** to use the **SSH** service.

```
[Device-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

Verifying the configuration

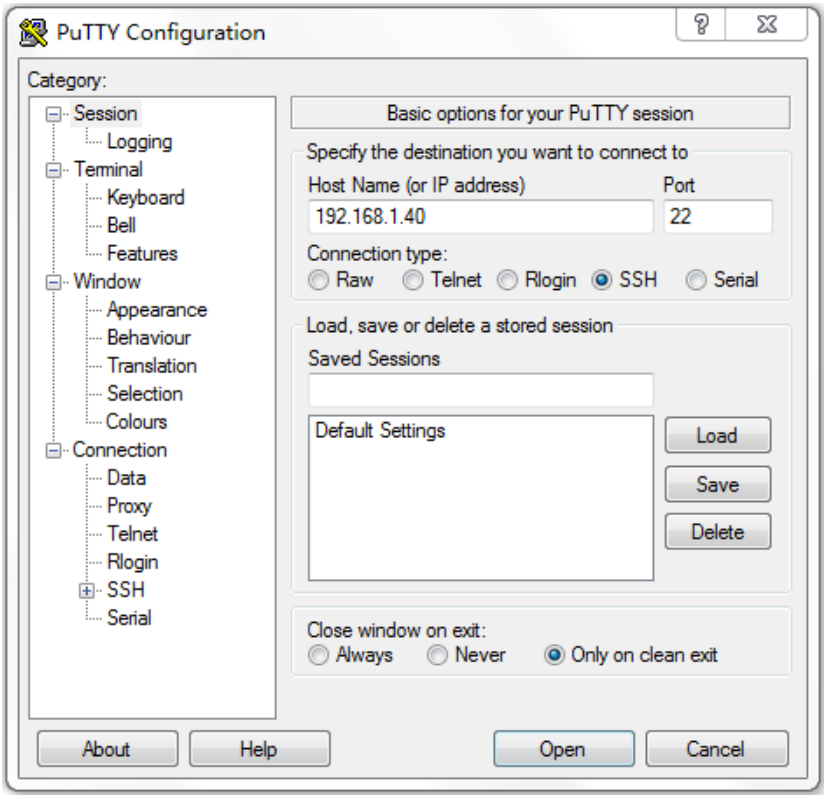
There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs Putty version 0.60.

To verify that you can log in to the Stelnet server from the Stelnet client:

1. Launch PuTTY.exe.
2. From the navigation tree, click **Session**.

   The interface shown in Figure 2 appears.
3. In the **Specify the destination you want to connect to** area, configure the following parameters:
   a. Enter **192.168.1.40** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Connection type**.

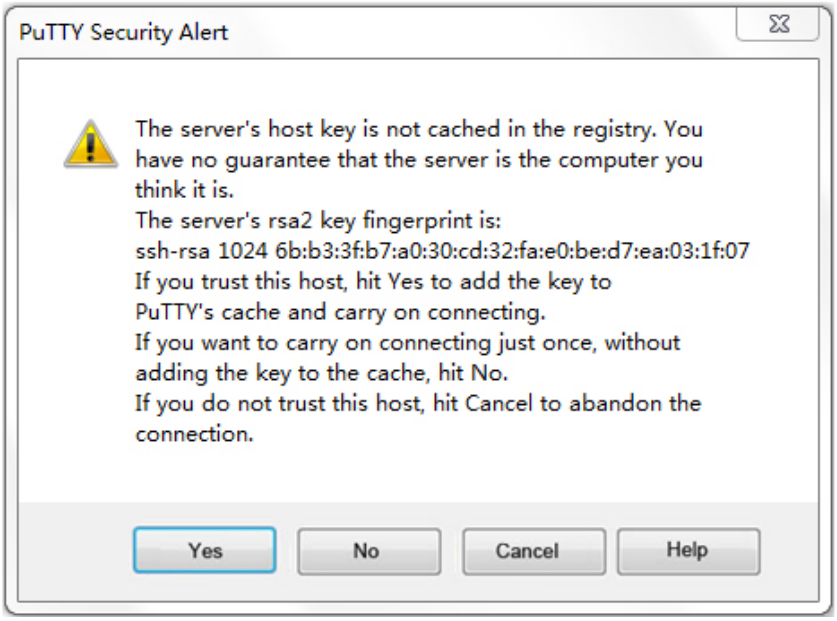
Figure 2 Specifying basic connection parameters



4. Click **Open**.

   The **PuTTY Security Alert** dialogue box appears.

   Figure 3 PuTTY Security Alert dialogue box



5. Click **Yes**.
6. Enter the username **client001** and the password **hello12345** to log in to the Stelnet server.

```
login as: client001
```

```
client001@192.168.1.40's password:

******************************************************************************
*Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001 class manage
 password hash $h$6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZIpSNi9b
cBEXhpvIqaYTvIVBf7ZUNGnovFsqW7nYxjoToRDvYBg==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

Example: Configuring the device as an Stelnet server using publickey authentication

Network configuration

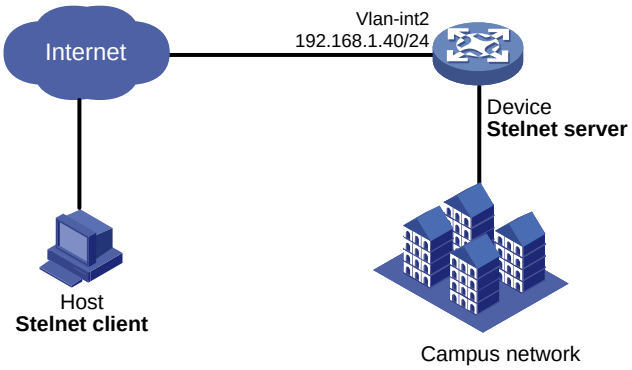
As shown in Figure 4:

- The device uses publickey authentication and RSA public key algorithm.
- The login username is **client001**.

Establish an Stelnet connection between the host and the device, so you can log in to the device to manage the campus network.

Import the client's host public key to the server to ensure correct format and content of the public key.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the server.
- For successful publickey authentication, perform the following tasks:
  a. Configure the client's RSA host public key on the server.
  b. Specify the paired RSA host private key for the SSH user on the client.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).
- To assign correct working directory and user role to the SSH user, you must create a local user on the Stelnet server. The local user must have the same username as the SSH user. To enable an SSH user to use all commands after login, set the user role of the local user to network-admin. By default, the user role of a local user is network-operator.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release

Hardware	Software version
	6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

Hardware	Software version
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

When you configure the device as an Stelnet server using publickey authentication, follow these restrictions and guidelines:

- In FIPS mode, the Stelnet server does not support publickey authentication.
- To support Stelnet clients that use different types of key pairs, generate DSA and RSA key pairs on the Stelnet server.

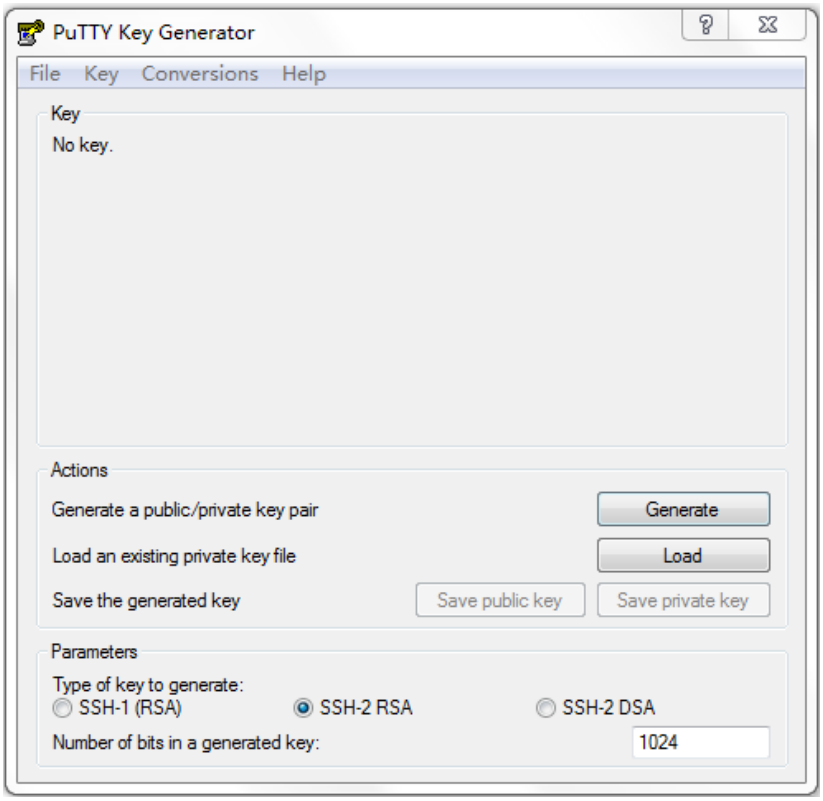
Procedures

Configuring the host as an Stelnet client

There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs Putty version 0.60.

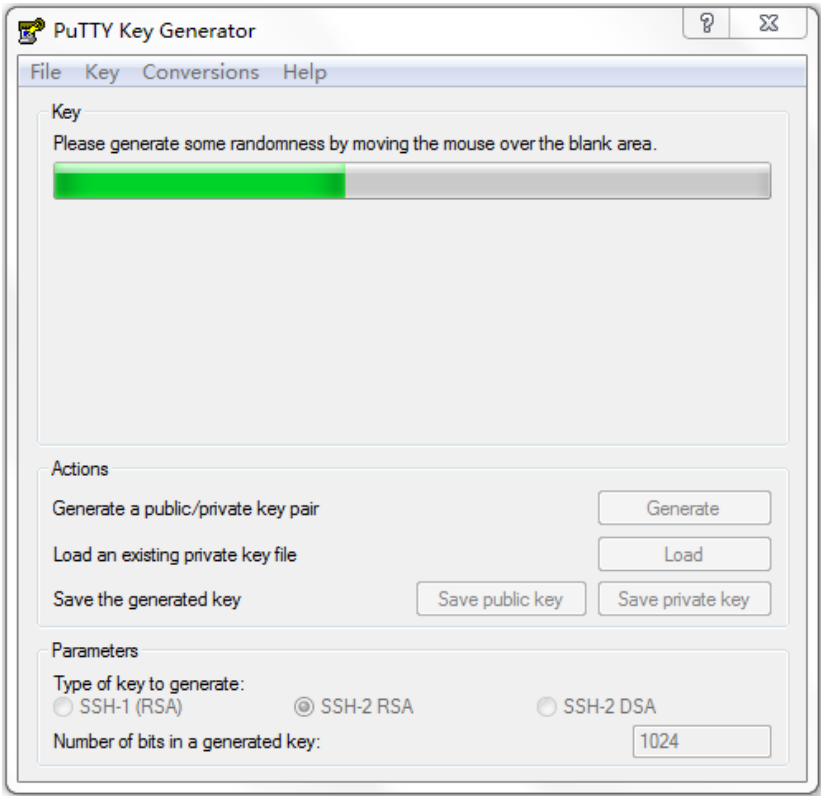
1. Run PuTTYGen.exe, select **SSH-2 RSA**, and click **Generate**.

   Figure 5 Generating a key pair on the client



2. Continuously move the mouse and do not place the mouse over the green process bar shown in Figure 6. Otherwise, the process bar stops moving and the key pair generating process stops.

Figure 6 Generating process

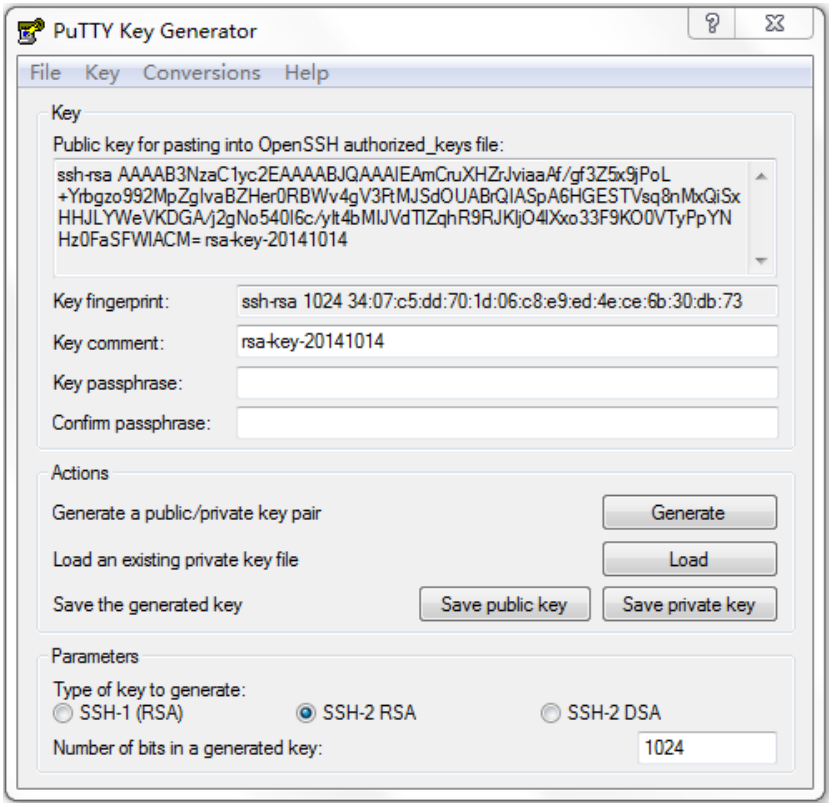


3. After the key pair is generated, click **Save public key**.

   A file saving window appears.

4. Select the saving directory (disk D in this example), enter a file name (**key.pub** in this example), and click **Save**.

Figure 7 Saving a key pair on the client



5. On the page shown in Figure 7, click **Save private key**.

   A confirmation dialog box appears.

6. Click **Yes**.

   A file saving window appears.

7. Select the saving directory (disk D in this example), enter a file name (**private.ppk** in this example), and click **Save**.

Configuring the device as the FTP server

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Device-Vlan-interface2] quit
```

Create a local user **ftp**.

```
[Device] local-user ftp class manage
New local user added.
```

Set the password to **hello12345** in plain text for the local user **ftp**.

```
[Device-luser-manage-ftp] password simple hello12345
```

Assign the user role **network-admin** to the local user **ftp**.

```
[Device-luser-manage-ftp] authorization-attribute user-role network-admin
```

Assign the working directory **flash:/** to the local user **ftp**.

```
[Device-luser-manage-ftp] authorization-attribute work-directory flash:/
```

Authorize the local user **ftp** to use the **FTP** service.

```
[Device-luser-manage-ftp] service-type ftp
[Device-luser-manage-ftp] quit
```

Enable the FTP server function.

```
[Device] ftp server enable
[Device] quit
```

Uploading the public key file from the FTP client

On the host, execute the cmd command **C:\Windows\system32>D:** to enter the D drive of the host.

Log in to the FTP server from the host and upload the public key file **key.pub** to the server.

```
ftp> put key.pub
200 PORT command successful
150 Connecting to port 62399
226 File successfully transferred
```

Configuring the device as the Stelnet server

Generate RSA key pairs.

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate a DSA key pair.

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the SSH server function.

```
[Device] ssh server enable
```

Set the authentication mode to AAA (**scheme**) for the user lines.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

Import the client's public key from the file **key.pub**, and name the public key **devicekey**.

```
[Device] public-key peer devicekey import sshkey key.pub
```

Create an SSH user **client001**. Specify the authentication type as **publickey** for the user, and assign the public key **devicekey** to the user.

```
[Device] ssh user client001 service-type stelnet authentication-type publickey assign
publickey devicekey
```

Create a local user **client001**.

```
[Device] local-user client001 class manage
New local user added.
```

Authorize the local user **client001** to use the **SSH** service.

```
[Device-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[Device-luser-manage-client001] authorization-attribute user-role network-admin
[Device-luser-manage-client001] quit
```

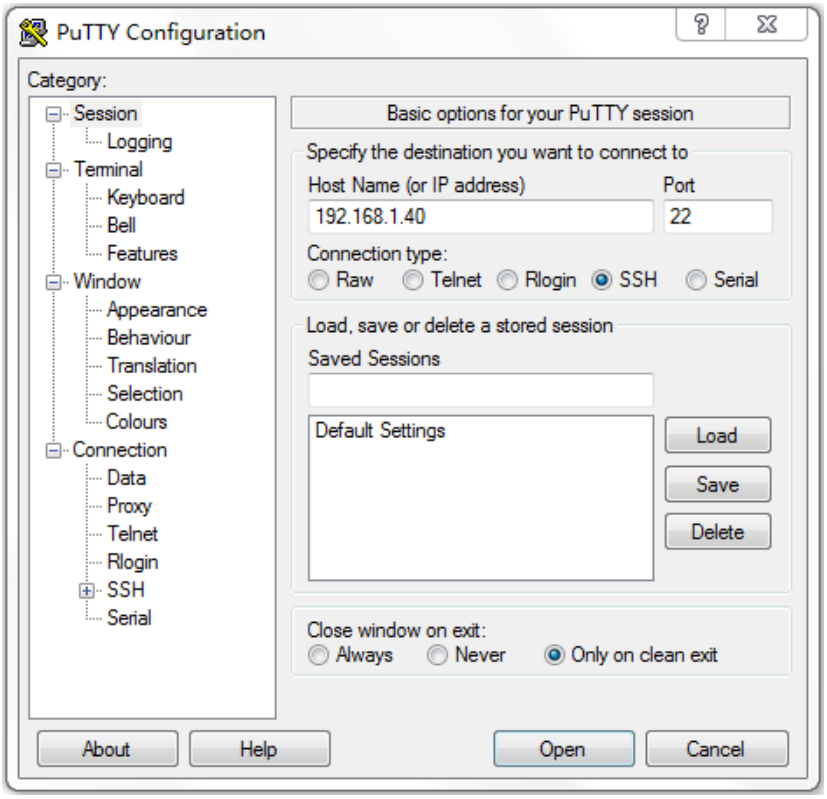
Verifying the configuration

To verify that you can log in to the Stelnet server from the Stelnet client:

1. Launch PuTTY.exe.
2. From the navigation tree, click **Session**.

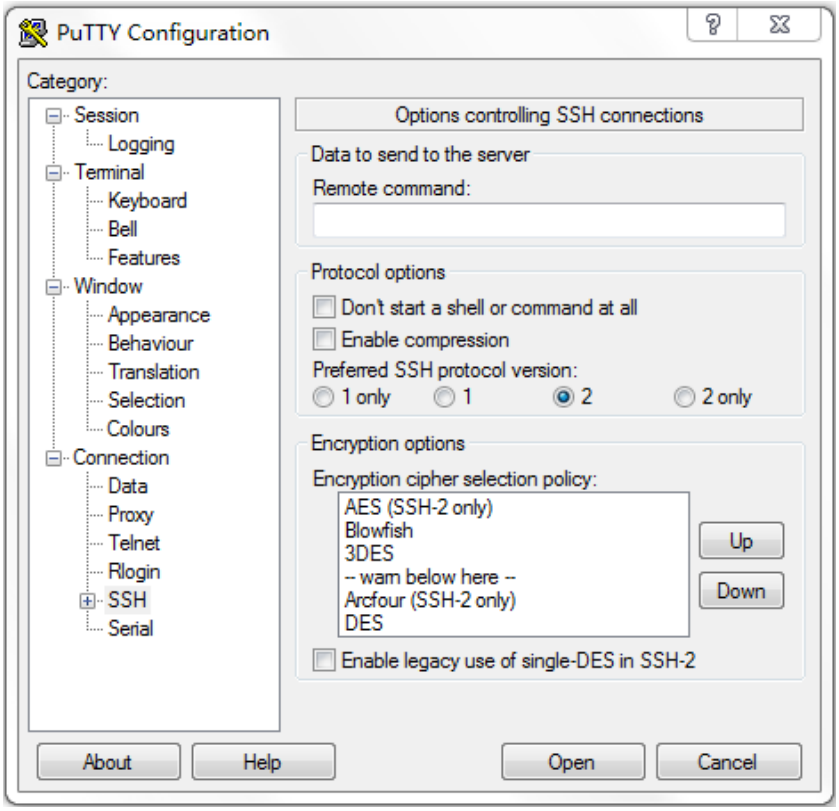
   The interface shown in Figure 8 appears.
3. In the **Specify the destination you want to connect to** area, configure the following parameters:
   a. Enter **192.168.1.40** in the **Host Name (or IP address)** field.
   b. Enter **22** in the **Port** field.
   c. Select **SSH** for **Connection type**.

Figure 8 Specifying basic connection parameters



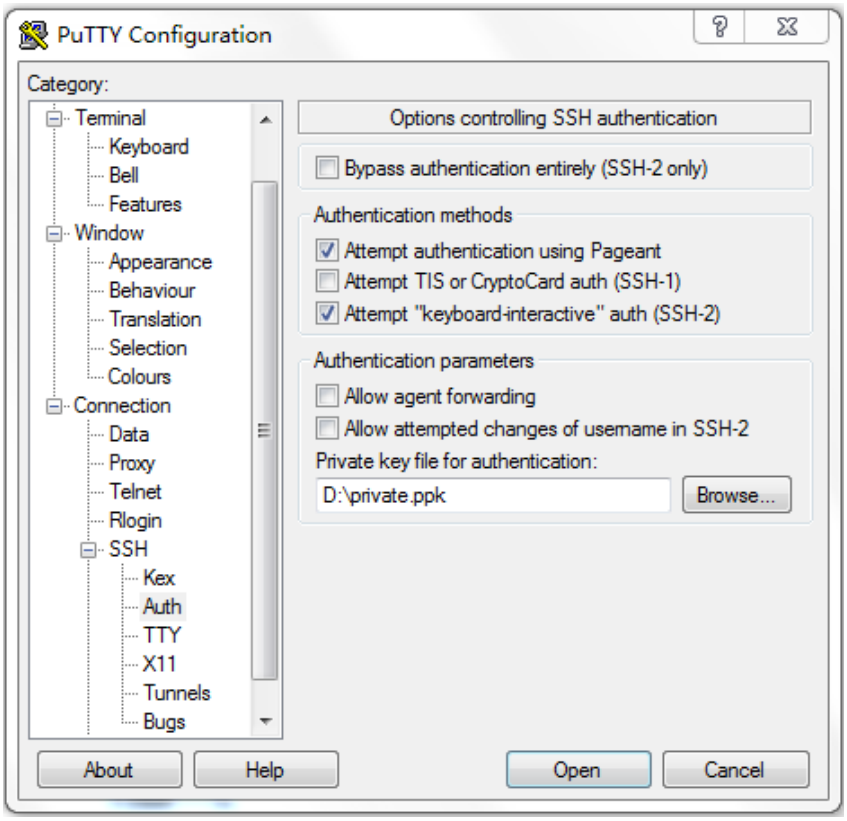
4. From the navigation tree, select **Connection** > **SSH**.
   The window shown in Figure 10 appears.
5. In the **Protocol options** area, specify the preferred SSH version as 2.

Figure 9 Specifying the SSH version



6. From the navigation tree, select **Connection** > **SSH** > **Auth**.
   The window shown in Figure 10 appears.
7. Click **Browse…**.
   A file selection window appears.
8. Select the private key file **private.ppk**, and click **OK**.

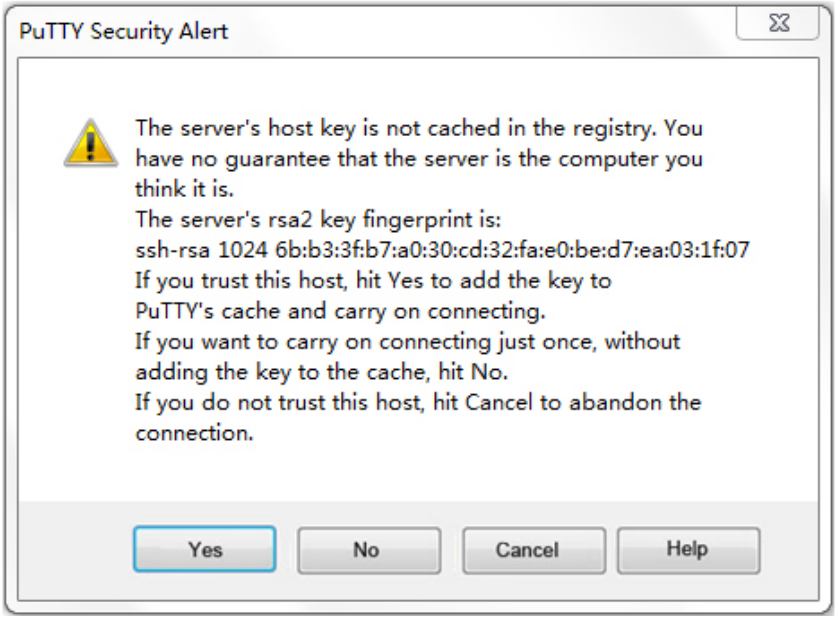
Figure 10 Specifying the private key file



9. Click **Open**.

   The **PuTTY Security Alert** dialogue box appears.

   Figure 11 PuTTY Security Alert dialogue box



10. Click **Yes**.
11. Enter the username **client001** to log in to the Stelnet server.

```
login as: client001
```

```
Authenticating with public key ”rsa-key-20140726”

******************************************************************************
*Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 line vty 0 63
 authentication-mode scheme
#
ssh server enable
ssh user client001 service-type stelnet authentication-type publickey assign publickey
devicekey
#
local-user client001 class manage
service-type ssh
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
public-key peer Devicekey
public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837BEF5D32259844
2D6753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A6627243EAD766D57AEA70B901B4B45
66D9A651B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCAF28FF21EE4EADAE6DF52001944A40414DFF2
80FF043B14838288BE7F9438DC71ABBC2C28BF78F34ADF3D1C912579A19020125
public-key-code end
peer-public-key end
#
local-user ftp
password cipher $c$3$sg9WgqO1w8vnAv2FKGTOYgFJm3nn2w==
```

```
authorization-attribute work-directory flash:/
authorization-attribute user-role network-operator
service-type ftp
#
ftp server enable
#
```

Example: Configuring the device as an Stelnet client for password authentication

Network configuration

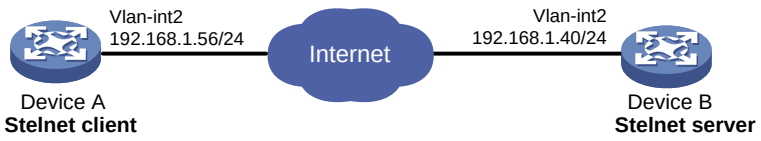
As shown in Figure 12:

- Device B uses local password authentication.
- The login username and password are **client001** and **hello12345**, respectively.

Establish an Stelnet connection between Device A and Device B, so you can log in to Device B to use all commands and perform secure data exchange.

To ensure communication security, configure Device A to use the host public key of Device B to authenticate Device B.

Figure 12 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA and RSA key pairs on the server.
- The authentication mode for Stelnet user lines must be AAA (**scheme**).
- To perform local authentication, create a local user and configure a password for the local user on the Stelnet server.
- To enable an SSH user to use all commands after login, set the user role of the local user to network-admin. By default, the user role of a local user is network-operator.
- Because the Stelnet client uses the host public key of the server to authenticate the server, you must configure the host public key of the server on the client.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

Configuring the Stelnet server

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate a DSA key pair.

```
[DeviceB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[DeviceB] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the SSH server function.

```
[DeviceB] ssh server enable
```

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The Stelnet client uses this address as the destination address of the Stelnet connection.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[DeviceB-Vlan-interface2] quit
```

Set the authentication mode to AAA (**scheme**) for the user lines.

```
[DeviceB] line vty 0 63
[DeviceB-line-vty0-63] authentication-mode scheme
[DeviceB-line-vty0-63] quit
```

Create a local user **client001**.

```
[DeviceB]local-user client001 class manage
New local user added.
```

Set the password to **hello12345** in plain text for the local user **client001**.

```
[DeviceB-luser-manage-client001] password simple hello12345
```

Authorize the local user **client001** to use the **SSH** service.

```
[DeviceB-luser-manage-client001]service-type ssh
```

Assign the user role **network-admin** to the local user **client001**.

```
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
[DeviceB-luser-manage-client001]quit
```

Display the DSA key pair of the server.

```
[DeviceB] display public-key local dsa public

=====================================================
Key name: dsakey (default)
Key type: DSA
Key length: 1024
Time when key pair created: 11:02:10 2016/07/07
Key code:

   308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

Configuring the Stelnet client

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The client uses this IP address to connect to the server.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[DeviceA-Vlan-interface2] quit
```

Specify the name of the server's host public key as **key1** and enter public key view.

```
[DeviceA] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
```

Configure the host public key of the Stelnet server by entering the public key displayed by the **`display public-key local dsa public`** command. By default, the client authenticates the server by using the DSA host public key of the server.

```
[DeviceA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F02818100D7572
62C4584C44C211F18BD96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C26585
4889DC1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD7
7FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B368950387811C7DA330215
00C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E14EC474BAF2932E69D3B1F1851
7AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5
B374E16DD00132CE71B020217091AC717B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E8
10561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F
4BE3F76FACBAB565AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55
A2C30A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872061F9B
4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
```

Exit public key view.

```
[DeviceA-pkey-public-key-key1] peer-public-key end
[DeviceA] return
```

Verifying the configuration

Verify that you can log in to the Stelnet server from the Stelnet client. The host public key of the server is **key1**.

```
<DeviceA> ssh2 192.168.1.40 publickey key1
login as: client001
client001@192.168.1.40's password:

******************************************************************************
*Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<DeviceB>
```

After you enter the username (**client001**) and the password (**hello12345**), you can log in to the Stelnet server successfully.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.1.56 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

```
public-key peer key1
public-key-code begin
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF03818400028180077F06B3E343CAE9988F4BE3F76FACBAB565
   AB73D4BA295C52BA92428B1F2DA1E6DD652413DD3AFE0C5A4FCF365100CBE34CECA55A2C30
   A2A9FF7E899628557E39CE8FC615F53193A7E200B4B1CB21E3F1091D595716D229DDED6872
   061F9B4B08301ADC81F7EC1501FFB863C0009536596CCB508596C3325892DC6D8C5C35B5
public-key-code end
peer-public-key end
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001
 password cipher $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
 service-type ssh
#
```

Example: Configuring SFTP with password-publickey authentication

Network configuration

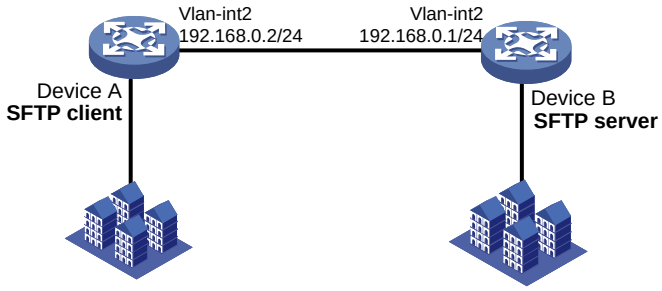
As shown in Figure 13:

- Device B uses password-publickey authentication and RSA public key algorithm.
- The login username and password are **client001** and **hello12345**, respectively.

Establish an SFTP connection between Device A and Device B, so you can log in to Device B to perform file and directory operations.

Import the client's host public key to the server to ensure correct format and content of the public key.

Figure 13 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Because the client's host public key is required in the server configuration, you must generate RSA key pairs on the client before configuring the SFTP server.
- For successful publickey authentication, perform the following tasks:
  a. Configure the client's RSA host public key on the server.
  b. Specify the paired RSA host private key for the SSH user on the client.

     To specify the RSA host private key on the client, use the **`identity-key rsa`** keyword in the **`sftp`** command.
- To perform local authentication, create a local user and configure a password for the local user on the SFTP server.
- To enable an SSH user to use all commands after login, set the user role of the local user to network-admin. By default, the user role of a local user is network-operator.
- To assign correct working directory and user role to the SSH user, configure the local user to have the same username as the SSH user.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx

Hardware	Software version
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series S5500V3-48P-SI switch series	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

Hardware	Software version
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

When you configure SFTP with password-publickey authentication, follow these restrictions and guidelines:

- In FIPS mode, the SFTP server does not support publickey authentication.
- To support SFTP clients that use different types of key pairs, generate DSA and RSA key pairs on the SFTP server.

Procedures

Configuring Device A as the SFTP client

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The client uses this address to connect to the server.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[DeviceA-Vlan-interface2] quit
```

Generate RSA key pairs.

```
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Export the host public key to the file **key.pub**.

```
[DeviceA] public-key local export rsa ssh2 key.pub
[DeviceA] quit
```

Configuring Device B as the FTP server

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[DeviceB-Vlan-interface2] quit
```

Create a local user **ftp**.

```
[DeviceB] local-user ftp class manage
New local user added.
```

Set the password to **hello12345** in plain text for the local user **ftp**.

```
[DeviceB-luser-manage-ftp] password simple hello12345
```

Assign the user role **network-admin** to the local user **ftp**.

```
[DeviceB-luser-manage-ftp] authorization-attribute user-role network-admin
```

Assign the working directory **flash:/** to the local user **ftp**.

```
[DeviceB-luser-manage-ftp] authorization-attribute work-directory flash:/
```

Authorize the local user **ftp** to use the **FTP** service.

```
[DeviceB-luser-manage-ftp] service-type ftp
[DeviceB-luser-manage-ftp] quit
```

Enable the FTP server function.

```
[DeviceB] ftp server enable
[DeviceB] quit
```

Uploading the public key file from the FTP client

Log in to the FTP server from Device A and upload the public key file **key.pub** to the server.

```
<DeviceA>ftp 192.168.0.1
Press CTRL+C to abort.
Connected to 192.168.0.1 (192.168.0.1).
220 FTP service ready.
User (192.168.0.2:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put flash:/key.pub
227 Entering Passive Mode (192,168,0,1,41,116)
150 Accepted data connection
226 File successfully transferred
301 bytes sent in 0.000 seconds (1.05 Mbytes/s)
ftp> quit
221-Goodbye. You uploaded 1 and downloaded 0 kbytes.
221 Logout.
```

Configuring Device B as the SFTP server

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate a DSA key pair.

```
[DeviceB] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
```

```
Generating Keys...
...
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[DeviceB] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Enable the SFTP server function.

```
[DeviceB] sftp server enable
```

Import the client's public key from the file **key.pub**, and name the public key **devicekey**.

```
[DeviceB] public-key peer devicekey import sshkey key.pub
```

Create an SSH user **client001**. Specify the authentication type as **password-publickey** for the user, and assign the public key **devicekey** to the user.

```
[DeviceB] ssh user client001 service-type sftp authentication-type password-publickey
assign publickey devicekey
```

Create a local user **client001**.

```
[DeviceB] local-user client001 class manage
New local user added.
```

Set the password to **hello12345** in plain text for the local user **client001**.

```
[DeviceB-luser-manage-client001] password simple hello12345
```

Authorize the local user **client001** to use the **SSH** service.

```
[DeviceB-luser-manage-client001] service-type ssh
```

Assign the user role **network-admin** and working directory **flash:/** to the local user **client001**.

```
[DeviceB-luser-manage-client001] authorization-attribute user-role network-admin
work-directory flash:/
[DeviceB-luser-manage-client001] quit
```

Verifying the configuration

1. Verify that you can log in to the SFTP server from the SFTP client.

   ```
   <DeviceA >sftp 192.168.0.1 identity-key rsa
   Username: client001
   Press CTRL+C to abort.
   Connecting to 192.168.0.1 port 22.
   The server is not authenticated. Continue? [Y/N]:y
   Do you want to save the server public key? [Y/N]:n
   client001@192.168.0.1's password:
   ```

   After you enter the password, you are placed in SFTP client view.

   ```
   sftp>
   ```

2. Verify that you can perform file and directory operations after logging in to the SFTP server:

   # Display files under the current directory of the server, delete the file **z**, and verify the result.

   ```
   sftp> dir -l
   -rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
   -rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
   -rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
   ```

```
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 1        1                0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

Add a directory **new1** and verify the result.

```
sftp> mkdir new1
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:30 new1
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

Rename directory **new1** to **new2** and verify the result.

```
sftp> rename new1 new2
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
```

Download the file **pubkey2** from the server and change the name to **public**.

```
sftp> get pubkey2 public
Fetching /pubkey2 to public
/public                                       100%  301     0.3KB/s   00:00
```

Upload the local file **public** to the server, and verify the result.

```
sftp> put public
Uploading public to /public
public                                        100%  301     0.3KB/s   00:00
sftp> dir -l
-rwxrwxrwx    1 1        1             1759 Aug 23 06:52 config.cfg
-rw-rw----    1 1        1              301 Aug  7 16:52 key.pub
-rwxrwxrwx    1 1        1                0 Sep 01 06:22 new
drwxrwxrwx    1 1        1                0 Sep 02 06:33 new2
-rwxrwxrwx    1 1        1              225 Sep 01 06:55 pub
-rwxrwxrwx    1 1        1              225 Aug 24 08:01 pubkey2
-rwxrwxrwx    1 1        1              301 Jul 30 16:21 public
sftp>
```

Exit SFTP client view.

```
sftp> quit
```

```
<DeviceA>
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.0.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
sftp server enable
ssh user client001 service-type sftp authentication-type password-publickey assign
publickey devicekey
#
local-user client001 class manage
service-type ssh
password cipher $c$3$o71Exx1XIKs9gJoxqSodHGl1uT9rlZEd4w==
 authorization-attribute user-role network-operator
 authorization-attribute user-role network-admin
#
ftp server enable
#
local-user ftp class manage
 password simple ftp
 service-type ftp
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
public-key peer devicekey
```

```
 public-key-code begin
30819F300D06092A864886F70D010101050003818D00308189
1BD316C0DBB9009503E78F31947B651F9950E9A6E9E256E1E
 public-key-code end
 peer-public-key end
#
```

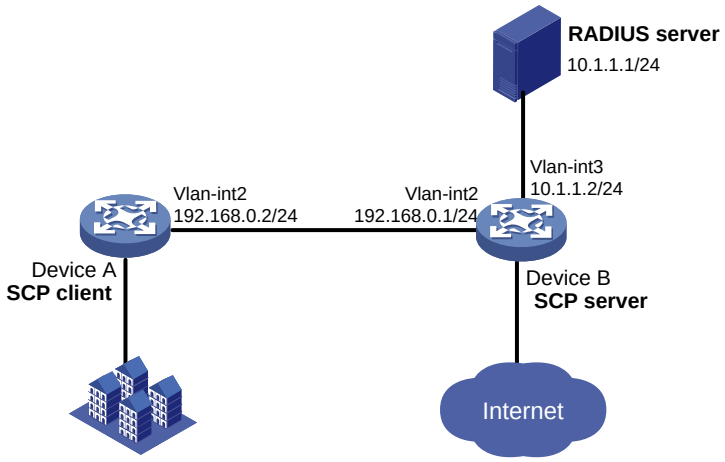
Example: Configuring SCP file transfer with remote password authentication

Network configuration

As shown in Figure 14, configure the devices and the RADIUS server to meet the following requirements:

- Establish an SCP connection between Device A and Device B, so you can log in to Device B to perform file transfer.
- Use the RADIUS server for SSH user authentication and authorization. The user name and password are **hello@bbb** and **hello12345**, respectively.
- Include the domain name in the username sent to the RADIUS server.
- Assign the default user role **network-admin** to the SSH user, so the user can use all commands after login.

Figure 14 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To ensure correct SSH version negotiation and algorithm negotiation, and to ensure that the server can pass the client's authentication, generate DSA and RSA key pairs on the SSH server.
- To perform remote password authentication, configure the username and password on the RADIUS server. To enable an SSH user to use all commands after login, set the user role to **network-admin** for the user on the RADIUS server.

- To use the RADIUS server for authentication and authorization, perform the following tasks on Device B:
  a. Configure a RADIUS scheme to specify the authentication and authorization server.
  b. Create an ISP domain, and specify the ISP domain to use the RADIUS scheme for authentication, authorization, and accounting.
- To ensure communication security between the RADIUS client (Device B) and the RADIUS server, configure the same shared key on Device B and the RADIUS server.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch series	Release 63xx

Hardware	Software version
S5500V3-48P-SI switch series	
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx

Hardware	Software version
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Procedures

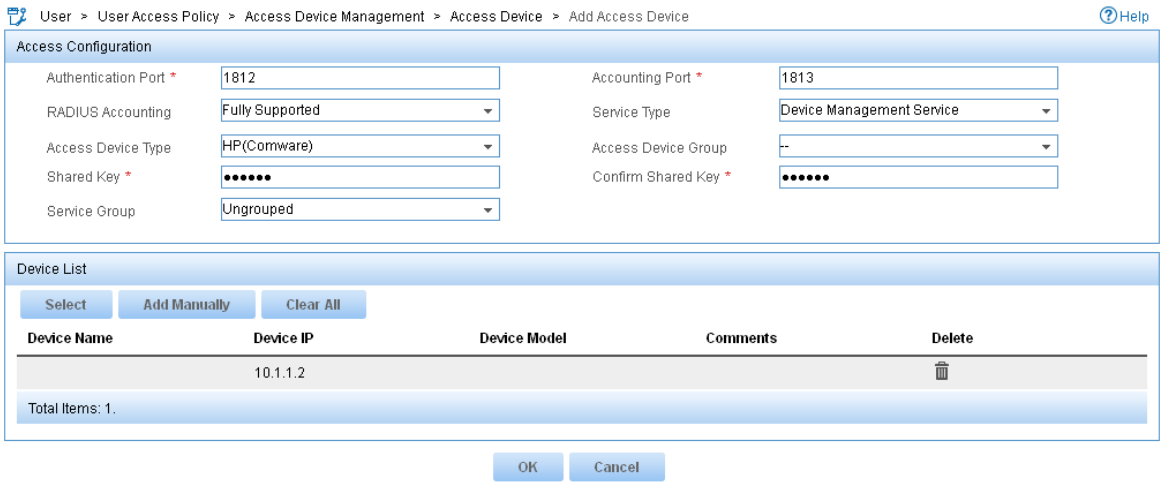
Configuring the RADIUS server

In this example, the RADIUS server runs on IMC PLAT 7.0 (E0102) and IMC UAM 7.0 (E0201).

Adding Device B to the IMC Platform as an access device

1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation tree, select **User Access Policy**> **Access Device Management** > **Access Device**.
4. Click **Add**.
5. Configure an access device as follows:
   a. Set the ports for authentication and accounting to **1812** and **1813**, respectively.
   b. Select the service type **Device Management Service**.
   c. Select the access device type **HP(Comware)**.
   d. Set the shared key to **expert** for secure RADIUS communication.
   e. Select Device B from the device list or manually add Device B. (The IP address of Device B is 10.1.1.2).
   f. Use the default settings for other parameters.
6. Click **OK**.

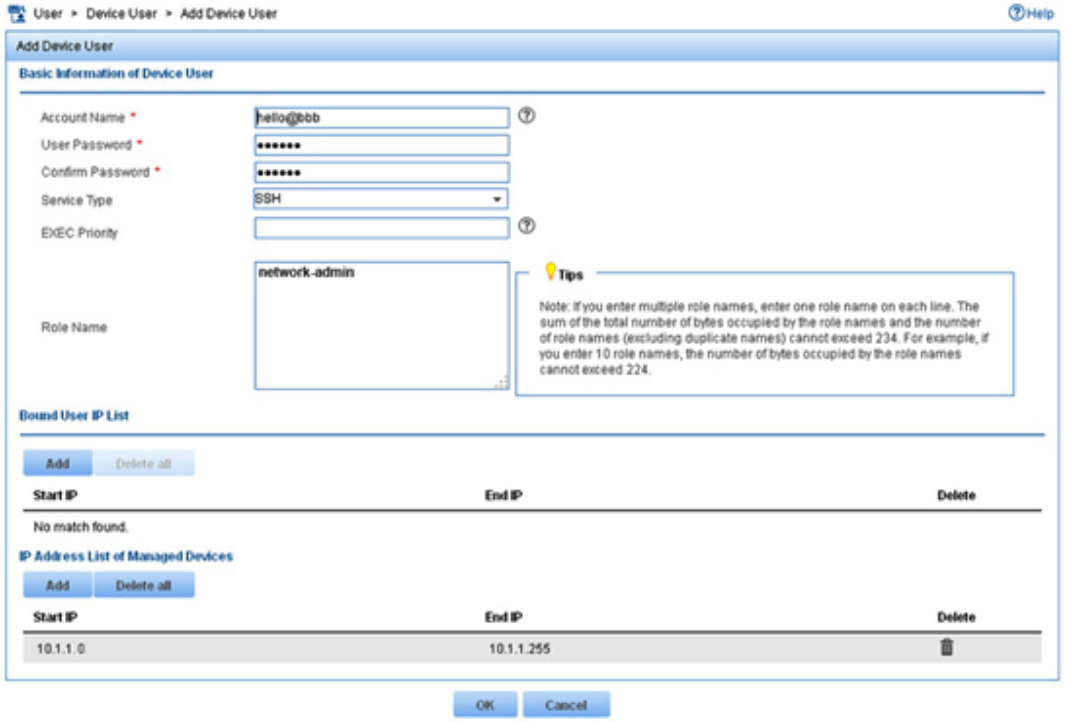
Figure 15 Adding Device B as an access device



Adding an account for device management

1. Click the **User** tab.
2. From the navigation tree, select **Access User** > **Device User**.
3. Click **Add**.
4. Configure a device management account as follows:
   a. Enter the account name **hello@bbb** and the password **hello12345**.
   b. Select the service type **SSH**.
   c. Enter the user role **network-admin** in the **Role Name** field.
   d. Specify **10.1.1.0** to **10.1.1.255** as the IP address range of the devices to be managed.
5. Click **OK**.

Figure 16 Adding a device management account



Configuring Device B

Generate RSA key pairs.

```
<DeviceB> system-view
[DeviceB] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate a DSA key pair.

```
[DeviceB] public-key local create dsa
```

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

Generate an ECDSA key pair.

```
[DeviceB] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/2
[DeviceB-vlan2] quit
```

Assign an IP address to VLAN-interface 2. The SCP client uses this address as the destination IP address of the SCP connection.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[DeviceB-Vlan-interface2] quit
```

Create VLAN 3, and assign GigabitEthernet 1/0/3 to VLAN 3.

```
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/3
[DeviceB-vlan3] quit
```

Assign an IP address to VLAN-interface 3. Device B uses this address to communicate with the RADIUS server.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[DeviceB-Vlan-interface3] quit
```

Enable the SSH server function.

```
[DeviceB] ssh server enable
```

Create a RADIUS scheme **rad**.

```
[DeviceB] radius scheme rad
```

Specify the primary authentication server 10.110.1.1 and UDP port 1812 for the RADIUS scheme **rad**.

```
[DeviceB-radius-rad] primary authentication 10.1.1.1 1812
```

Specify the primary authentication server 10.110.1.1 and UDP port 1813 for the RADIUS scheme **rad**.

```
[DeviceB-radius-rad] primary accounting 10.1.1.1 1813
```

Specify the shared key as **expert** for secure authentication and accounting communication.

```
[DeviceB-radius-rad] key authentication simple expert
[DeviceB-radius-rad] key accounting simple expert
```

Include domain names in the usernames sent to the RADIUS server.

```
[DeviceB-radius-rad] user-name-format with-domain
[DeviceB-radius-rad] quit
```

Create an ISP domain **bbb**.

```
[DeviceB] domain bbb
```

Configure ISP domain **bbb** to use RADIUS scheme **rad** for authentication, authorization, and accounting of all login users.

```
[DeviceB-isp-bbb] authentication login radius-scheme rad
[DeviceB-isp-bbb] authorization login radius-scheme rad
[DeviceB-isp-bbb] accounting login radius-scheme rad
[DeviceB-isp-bbb] quit
```

Configuring Device A

Create VLAN 2, and assign GigabitEthernet 1/0/2 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/2
[DeviceA-vlan2] quit
```

Assign an IP address to VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[DeviceA-Vlan-interface2] quit
[DeviceA] quit
```

Verifying the configuration

Verify that you can log in to the SCP server, download the file **remote.bin** from the server, and save it locally with the name **local.bin**.

```
<DeviceA> scp 192.168.0.1 get remote.bin local.bin
Username: hello@bbb
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
hello@bbb@192.168.0.1's password:
remote.bin                    100% 8275KB 318.3KB/s   00:26.
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.0.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- Device B:

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$63G7LzIQElGq4aFGTiYQafU+loQxS/cbLg==
 key accounting cipher $c$3$tUIVlyGISJ5X/yiTFWrmh8nyjBIF+1LFzQ==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

Contents

Introduction

This document provides IP source guard (IPSG) configuration examples.

IPSG prevents spoofing attacks by using IPSG bindings to filter incoming packets. IPSG bindings include static bindings that are configured manually and dynamic bindings that are generated based on information from modules such as DHCP. IPSG forwards only the packets that match IPSG bindings.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IPSG.

Example: Configuring static IPv4SG

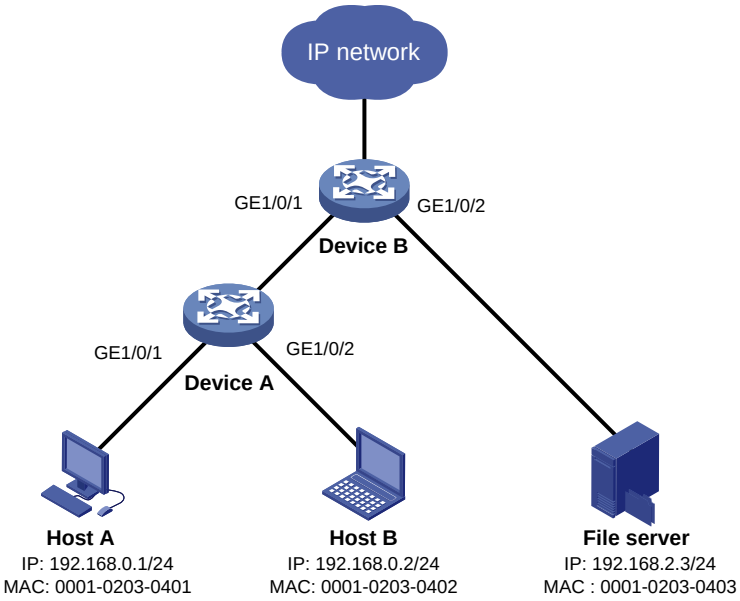
Network configuration

As shown in Figure 1, Host A, Host B, and the file server use static IPv4 addresses.

Enable static IPv4SG and configure static IPSG bindings on Device A and Device B to meet the following requirements:

- The interface GigabitEthernet 1/0/1 of Device A allows IP packets from Host A to pass.
- All interfaces of Device A allow IP packets from Host B to pass.
- The interface GigabitEthernet 1/0/1 of Device B allows only IP packets from Host A and Host B to pass.
- The interface GigabitEthernet 1/0/2 of Device B allows only IP packets from the file server to pass.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To allow IP packets from Host A to pass through GigabitEthernet 1/0/1 on Device A, configure a static IPSG binding for Host A on the interface.
- To allow IP packets from Host B to pass through all interfaces on Device A, configure a global static IPSG binding for Host B.
- To allow IP packets from both hosts to pass through GigabitEthernet 1/0/1 on Device B, configure static IPSG bindings for the hosts on the interface.
- To allow only IP packets from the file server to pass through GigabitEthernet 1/0/2 on Device B, configure a static IPSG binding for the file server on the interface.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx,

Hardware	Software version
	Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series	Release 63xx

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

IPSG does not use the VLAN information (if specified) in static IPSG bindings to filter packets.

Procedures

Configuring Device A

Create VLAN 10, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/2 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceA-vlan10] quit
```

Create VLAN-interface 10, and assign an IP address to VLAN-interface 10.

```
[DeviceA] interface vlan-interface 10
```

```
[DeviceA-Vlan-interface10] ip address 192.168.0.10 255.255.255.0
[DeviceA-Vlan-interface10] quit
```

Enable IPv4SG on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Configure a static IPSG binding for Host A on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0401
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure a static IPSG binding for Host B.

```
[DeviceA] ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0402
```

Configuring Device B

Create VLAN 10, and assign GigabitEthernet 1/0/1 to VLAN 10.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port gigabitethernet 1/0/1
[DeviceB-vlan10] quit
```

Create VLAN-interface 10, and assign an IP address to VLAN-interface 10.

```
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] ip address 192.168.0.100 255.255.255.0
[DeviceB-Vlan-interface10] quit
```

Create VLAN 20, and assign GigabitEthernet 1/0/2 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

Create VLAN-interface 20, and assign an IP address to VLAN-interface 20.

```
[DeviceB] interface vlan-interface 20
[DeviceB-Vlan-interface20] ip address 192.168.2.100 255.255.255.0
[DeviceB-Vlan-interface20] quit
```

Enable IPv4SG on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Configure static IPSG bindings for Host A and Host B on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0401
[DeviceB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2 mac-address
0001-0203-0402
[DeviceB-GigabitEthernet1/0/1] quit
```

Enable IPSG on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

Configure a static IPSG binding for the file server on GigabitEthernet 1/0/2.

```
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.2.3 mac-address
0001-0203-0403
[DeviceB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that Host A can ping the IP addresses of GigabitEthernet 1/0/1 on both Device A and Device B. (Details not shown.)

Verify that Host B can ping the IP addresses of all interfaces of Device A and GigabitEthernet 1/0/1 of Device B. (Details not shown.)

Verify that the file server can ping the IP address of VLAN-interface 20 of Device B. (Details not shown.)

Verify that Device A has static IPSG bindings for Host A and Host B.

```
[DeviceA] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.2     0001-0203-0402 N/A                     N/A  Static
192.168.0.1     0001-0203-0401 GE1/0/1                 N/A  Static
```

Verify that Device B has static IPSG bindings for Host A, Host B, and the file server.

```
[DeviceB] display ip source binding static
Total entries found: 3
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0401 GE1/0/1                 N/A  Static
192.168.0.2     0001-0203-0402 GE1/0/1                 N/A  Static
192.168.2.3     0001-0203-0403 GE1/0/2                 N/A  Static
```

Verify that Host B can ping Device A when Host B is connected to Device A through GigabitEthernet 1/0/1. (Details not shown.)

Verify that Host B cannot ping Device A when Host B is assigned an IP address different from 192.168.0.2. (Details not shown.)

Verify that Host A cannot ping Device A when any of following conditions exist (details not shown):

- Host A is connected to Device A through GigabitEthernet 1/0/2 or GigabitEthernet 1/0/3.
- Host A is assigned an IP address different from 192.168.0.1.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0402
#
vlan 10
#
interface Vlan-interface10
 ip address 192.168.0.10 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0401
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 ip verify source ip-address mac-address
#
```

- Device B:

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0401
 ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0402
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.2.3 mac-address 0001-0203-0403
#
```

Example: Configuring dynamic IPv4SG based on DHCP snooping

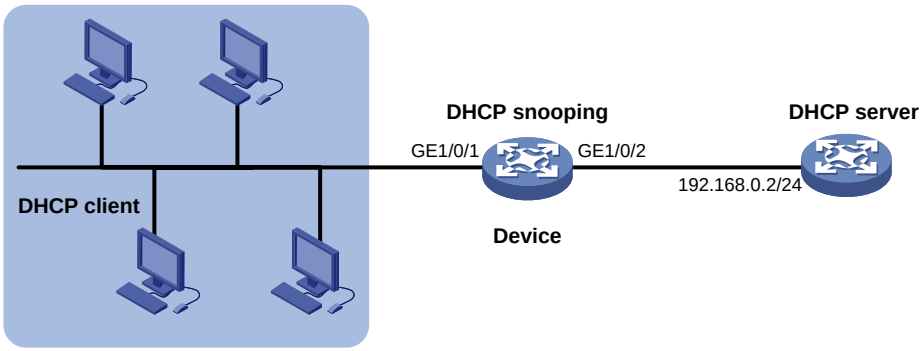
Network configuration

As shown in Figure 2, the DHCP clients obtain IP addresses from the DHCP server.

- Enable DHCP snooping on the device to make sure the DHCP clients obtain IP addresses from the authorized DHCP server.

- Enable dynamic IPv4SG on GigabitEthernet 1/0/1 to filter incoming packets by using the IPSG bindings that are generated based on DHCP snooping entries. Only packets from the DHCP clients are allowed to pass.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To enable the DHCP clients to obtain IP addresses from the DHCP server, configure GigabitEthernet 1/0/2 as the DHCP trusted port. By default, all ports are untrusted ports after DHCP snooping is enabled.
- To generate DHCP snooping entries for the DHCP clients, enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1. By default, recording of DHCP snooping entries is disabled.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-54C switch	
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series	Not supported

Hardware	Software version
S5000V5-EI switch series	
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

This example uses an S5560X-EI switch as the DHCP server.

Configuring the DHCP server

Create VLAN-interface 1, and assign an IP address to VLAN-interface 1.

```
<DHCPserver> system-view
[DHCPserver] interface vlan-interface 1
[DHCPserver-Vlan-interface1] ip address 192.168.0.2 24
```

Enable the DHCP server on VLAN-interface 1.

```
[DHCPserver-Vlan-interface1] dhcp select server
[DHCPserver-Vlan-interface1] quit
```

Enable DHCP.

```
[DHCPserver] dhcp enable
```

Create DHCP address pool 1.

```
[DHCPserver] dhcp server ip-pool 1
```

Specify the assignable subnet as 192.168.0.0/24 and the address lease duration as 7 days.

```
[DHCPserver-dhcp-pool-1] network 192.168.0.0 24
[DHCPserver-dhcp-pool-1] expired day 7
[DHCPserver-dhcp-pool-1] quit
```

Configuring the device

Enable DHCP snooping.

```
<Device> system-view
[Device] dhcp snooping enable
```

Configure GigabitEthernet 1/0/2 as a trusted port.

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] dhcp snooping trust
[Device-GigabitEthernet1/0/2] quit
```

Enable IPv4SG on GigabitEthernet 1/0/1 and verify the source IP address and MAC address for dynamic IPv4SG.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] dhcp snooping binding record
[Device-GigabitEthernet1/0/1] quit
```

Configuring the DHCP clients

Configure the DHCP clients to use DHCP for IP address acquisition. (Details not shown.)

Verifying the configuration

Verify that the device has generated dynamic IPSG bindings for the clients based on DHCP snooping entries.

```
[Device] display ip source binding dhcp-snooping
Total entries found: 4
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0401 GE1/0/1                 1    DHCP snooping
192.168.0.3     0001-0203-0403 GE1/0/1                 1    DHCP snooping
192.168.0.4     0001-0203-0404 GE1/0/1                 1    DHCP snooping
192.168.0.5     0001-0203-0405 GE1/0/1                 1    DHCP snooping
```

Verify that the DHCP server can be pinged from the clients. (Details not shown.)

Verify that the DHCP server cannot be pinged from the clients when the clients are assigned IP addresses manually. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
vlan 1
#
dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ip verify source ip-address mac-address
```

```
 dhcp snooping binding record
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 dhcp snooping trust
#
```

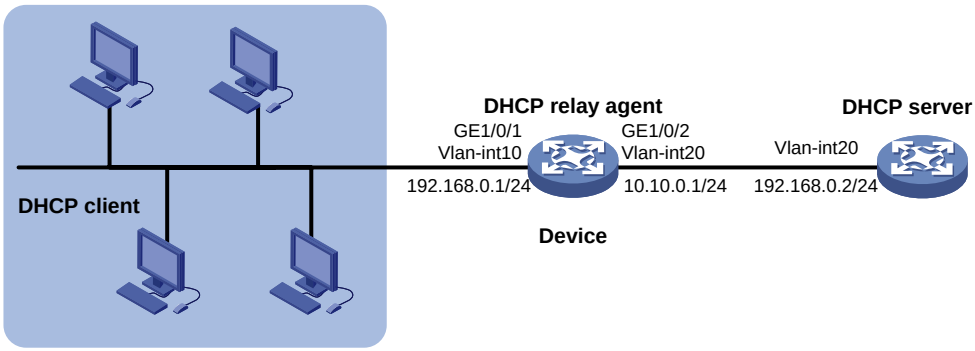
Example: Configuring dynamic IPv4SG based on DHCP relay agent

Network configuration

As shown in Figure 3, DHCP relay is enabled on the device. The DHCP clients obtain IP addresses from the DHCP server through the DHCP relay agent.

Enable dynamic IPv4SG on VLAN-interface 10 to filter incoming packets by using the dynamic IPSG bindings generated based on the DHCP relay entries.

Figure 3 Network diagram



Analysis

To generate DHCP relay entries for the DHCP clients, enable recording of relay entries on the delay agent. By default, the DHCP relay agent does not record client information in relay entries.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

Hardware	Software version
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx

Hardware	Software version
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

This example uses an S5560X-EI switch as the DHCP server.

Configuring the DHCP server

Create VLAN-interface 20, and assign an IP address to VLAN-interface 20.

```
<DHCPserver> system-view
[DHCPserver] interface vlan-interface 20
[DHCPserver-Vlan-interface20] ip address 10.10.0.2 24
```

Enable the DHCP server on VLAN-interface 20.

```
[DHCPserver-Vlan-interface20] dhcp select server
```

```
[DHCPserver-Vlan-interface20] quit
```

Enable DHCP.

```
[DHCPserver] dhcp enable
```

Create DHCP address pool 1.

```
[DHCPserver] dhcp server ip-pool 1
```

Specify the assignable subnet as 192.168.0.0/24 and the address lease duration as 7 days.

```
[DHCPserver-dhcp-pool-1] network 192.168.0.0 24
[DHCPserver-dhcp-pool-1] expired day 7
[DHCPserver-dhcp-pool-1] quit
```

Configure a static route for the subnet where VLAN-interface 10 of the DHCP relay agent resides on the DHCP server.

```
[DHCPserver] ip route-static 192.168.0.0 24 10.10.0.1
```

Configuring the device

Create VLAN 10, and assign GigabitEthernet 1/0/1 to VLAN 10.

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
```

Assign an IP address to VLAN-interface 10.

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 192.168.0.1 255.255.255.0
[Device-Vlan-interface10] quit
```

Create VLAN 20, and assign GigabitEthernet 1/0/2 to VLAN 20.

```
[Device] vlan 20
[Device-vlan20] port gigabitethernet 1/0/2
[Device-vlan20] quit
```

Assign an IP address to VLAN-interface 20.

```
[Device] interface vlan-interface 20
[Device-Vlan-interface20] ip address 10.10.0.1 255.255.255.0
[Device-Vlan-interface20] quit
```

Enable DHCP.

```
[Device] dhcp enable
```

Enable recording of relay entries on the delay agent.

```
[Device] dhcp relay client-information record
```

Enable the DHCP relay agent on VLAN-interface 10.

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] dhcp select relay
```

Specify the IP address of the DHCP server on the relay agent.

```
[Device-Vlan-interface10] dhcp relay server-address 10.10.0.2
[Device-Vlan-interface10] quit
```

Enable IPv4SG on VLAN-interface 10 and verify the source IP address and MAC address for dynamic IPSG.

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip verify source ip-address mac-address
[Device-Vlan-interface10] quit
```

Configuring the DHCP clients

Configure the DHCP clients to use DHCP for IP address acquisition. (Details not shown.)

Verifying the configuration

Verify that the device has generated dynamic IPSG bindings for the clients based on DHCP relay entries.

```
<Device> display ip source binding dhcp-relay
Total entries found: 4
IP Address      MAC Address    Interface               VLAN Type
192.168.0.2     0001-0203-0402 Vlan10                  10   DHCP relay
192.168.0.3     0001-0203-0403 Vlan10                  10   DHCP relay
192.168.0.4     0001-0203-0404 Vlan10                  10   DHCP relay
192.168.0.5     0001-0203-0405 Vlan10                  10   DHCP relay
```

Verify that the DHCP server can be pinged from the clients. (Details not shown.)

Verify that the DHCP server cannot be pinged from the clients when the clients are assigned IP addresses manually. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 dhcp enable
 dhcp relay client-information record
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.0.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 10.10.0.2
 ip verify source ip-address mac-address
#
interface Vlan-interface20
 ip address 10.10.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
```

#

Example: Configuring static IPv6SG and dynamic IPv6SG

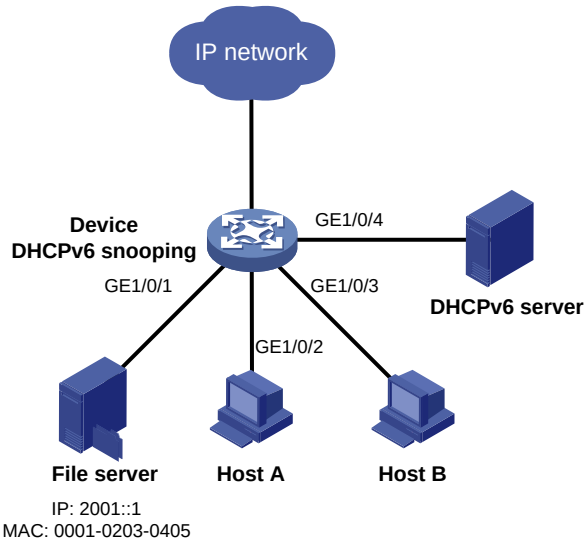
Network configuration

As shown in Figure 4, the file server uses static IPv6 address 2001::1. Host A and Host B obtain IP addresses from the DHCPv6 server.

Configure IPv6SG on the device to meet the following requirements:

- The interface GigabitEthernet 1/0/1 allows only packets from the file server to pass.
- The interface GigabitEthernet 1/0/2 allows only packets from Host A to pass.
- The interface GigabitEthernet 1/0/3 allows only packets from Host B to pass.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To enable Host A and Host B to obtain IP addresses from the DHCPv6 server, configure GigabitEthernet 1/0/4 as the DHCP trusted port. By default, all ports are untrusted ports after DHCPv6 snooping is enabled.
- To allow only incoming packets from the file server on GigabitEthernet 1/0/1, configure a static IPSG binding for the file server.
- To allow only packets from Host A to pass through GigabitEthernet 1/0/2 and only packets from Host B to pass through GigabitEthernet 1/0/3, perform the following tasks:
  - Enable IPv6SG on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.
  - To generate DHCPv6 snooping entries for Host A and Host B, enable recording of client information in DHCPv6 snooping entries on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. By default, recording of DHCP snooping entries is disabled.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

IPv6SG does not use the VLAN information (if specified) in static IPSG bindings to filter packets.

Procedures

Configure the DHCPv6 server and the DHCPv6 clients (Host A and Host B). (Details not shown.)

Enable IPv6SG on GigabitEthernet 1/0/1.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

Configure a static IPSG binding for the file server on GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0001-0203-0405
[Device-GigabitEthernet1/0/1] quit
```

Enable DHCPv6 snooping.

```
[Device] ipv6 dhcp snooping enable
```

Configure GigabitEthernet 1/0/4 as a trusted port.

```
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] ipv6 dhcp snooping trust
[Device-GigabitEthernet1/0/4] quit
```

Enable IPv6SG on GigabitEthernet 1/0/2 and verify the source IPv6 address and MAC address for dynamic IPv6SG.

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ipv6 verify source ip-address mac-address
```

Enable recording of client information in DHCPv6 snooping entries on GigabitEthernet 1/0/2.

```
[Device-GigabitEthernet1/0/2] ipv6 dhcp snooping binding record
[Device-GigabitEthernet1/0/2] quit
```

Enable IPv6SG on GigabitEthernet 1/0/3 and verify the source IPv6 address and MAC address for dynamic IPv6SG.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] ipv6 verify source ip-address mac-address
```

Enable recording of client information in DHCPv6 snooping entries on GigabitEthernet 1/0/3.

```
[Device-GigabitEthernet1/0/3] ipv6 dhcp snooping binding record
[Device-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Verify that the file server can ping the DHCPv6 server. (Details not shown.)

Verify that the device has a static IPSG binding for the file server.

```
[Device] display ipv6 source binding static
Total entries found: 1
IPv6 Address         MAC Address    Interface              VLAN Type
2001::1              0001-0203-0405 GE1/0/1                N/A  Static
```

Verify that the device has generated dynamic IPSG bindings for Host A and Host B based on DHCP snooping entries.

```
[Device] display ipv6 source binding dhcpv6-snooping
Total entries found: 2
IPv6 Address         MAC Address    Interface              VLAN Type
2001::2              0001-0203-0406 GE1/0/2                1    DHCPv6 snooping
2001::3              0001-0203-0407 GE1/0/3                1    DHCPv6 snooping
```

Verify that Host A and Host B can ping the DHCPv6 server. (Details not shown.)

Verify that Host A and Host B cannot ping the DHCPv6 server when they are assigned IPv6 addresses manually. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
ipv6 dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ipv6 verify source ip-address mac-address
 ipv6 source binding ip-address 2001::1 mac-address 0001-0203-0405
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 ipv6 verify source ip-address mac-address
 ipv6 dhcp snooping binding record
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 ipv6 verify source ip-address mac-address
 ipv6 dhcp snooping binding record
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 ipv6 dhcp snooping trust
#
```

Contents

Introduction

This document provides Ethernet OAM configuration examples.

Ethernet OAM is a tool that monitors the status of the link between two directly connected devices.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of Ethernet OAM.

Example: Configuring Ethernet OAM

Network configuration

As shown in Figure 1, the edge devices Device A and Device B connect the enterprise network and the carrier network. Configure Ethernet OAM on Device A and Device B to meet the following Service Level Agreement (SLA) requirements:

- Device A and Device B automatically monitor the link between them.
- The administrator can view critical link events on the link between Device A and Device B.
- The administrator can obtain the link status by observing link error event statistics.

Figure 1 Network diagram

Analysis

For Device A to establish an Ethernet OAM connection with Device B, configure GE 1/0/1 on Device A to operate in active mode, and configure GE 1/0/1 on Device B to operate in passive mode.

To implement link event detection based on the network environment, configure errored frame event detection parameters and use global settings for other detection parameters.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 series	Release 6615Pxx and Release 6628Pxx

S6813 series	
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

To change the Ethernet OAM mode on an Ethernet OAM-enabled port, first disable Ethernet OAM on the port.

Procedures

Configuring Device A

Configure GigabitEthernet 1/0/1 to operate in active Ethernet OAM mode (default mode), and enable Ethernet OAM for it.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode active
[DeviceA-GigabitEthernet1/0/1] oam enable
```

Set the errored frame event detection window to 20000 milliseconds, and set the errored frame event triggering threshold to 10 on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] oam errored-frame window 200
[DeviceA-GigabitEthernet1/0/1] oam errored-frame threshold 10
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Configure GigabitEthernet 1/0/1 to operate in passive Ethernet OAM mode, and enable Ethernet OAM for it.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] oam mode passive
[DeviceB-GigabitEthernet1/0/1] oam enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display Ethernet OAM configuration globally and on ports that do not use the default configuration.

```
[DeviceA] display oam configuration
---------------- [Global] ----------------
 OAM timers
   Hello timer        : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window           : 100 x 1000000 symbols
     Threshold        : 1 error symbols
   Errored frame
     Window           : 10 x 100 milliseconds
     Threshold        : 1 error frames
   Errored frame period
     Window           : 1000 x 10000 frames
     Threshold        : 1 error frames
   Errored frame seconds
     Window           : 600 x 100 milliseconds
     Threshold        : 1 error seconds
```

```
----------- [GigabitEthernet1/0/1] -----------
 OAM timers
   Hello timer        : 1000 milliseconds
   Keepalive timer    : 5000 milliseconds
 Link monitoring
   Errored symbol period
     Window           : 100 x 1000000 symbols
     Threshold        : 1 error symbols
   Errored frame
     Window           : 200 x 100 milliseconds
     Threshold        : 10 error frames
   Errored frame period
     Window           : 1000 x 10000 frames
     Threshold        : 1 error frames
   Errored frame seconds
     Window           : 600 x 100 milliseconds
     Threshold        : 1 error seconds
```

Display the statistics for critical Ethernet OAM link events that occurred on all ports of Device A.

```
[DeviceA] display oam critical-event
----------- [GigabitEthernet1/0/1] -----------
 Local link status   : UP
 Event statistics
   Link fault        : Not occurred
   Dying gasp        : Not occurred
   Critical event    : Not occurred
```

The output shows that no critical link event has occurred on the link between Device A and Device B.

Display Ethernet OAM link event statistics for the local end of Device A.

```
[DeviceA] display oam link-event local
----------- [GigabitEthernet1/0/1] -----------
 Link status: UP
 OAM local errored frame event
   Event time stamp        : 5789 x 100 milliseconds
   Errored frame window    : 200 x 100 milliseconds
   Errored frame threshold : 10 error frames
   Errored frame           : 13 error frames
   Error running total     : 350 error frames
   Event running total     : 17 events
```

The output shows the following information:

- 350 errors have occurred after Ethernet OAM is enabled on Device A.
- 17 errors are caused by error frames.
- The link is unstable.

NOTE:

If the link is unstable, contact HPE Support.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 oam errored-frame window 200
 oam errored-frame threshold 10
 oam enable
```

- Device B:

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 oam mode passive
 oam enable
```

Contents

Introduction

This document provides CFD configuration examples.

CFD is used for link connectivity detection, fault verification, and fault location in Layer 2 networks.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of CFD.

Example: Configuring CFD

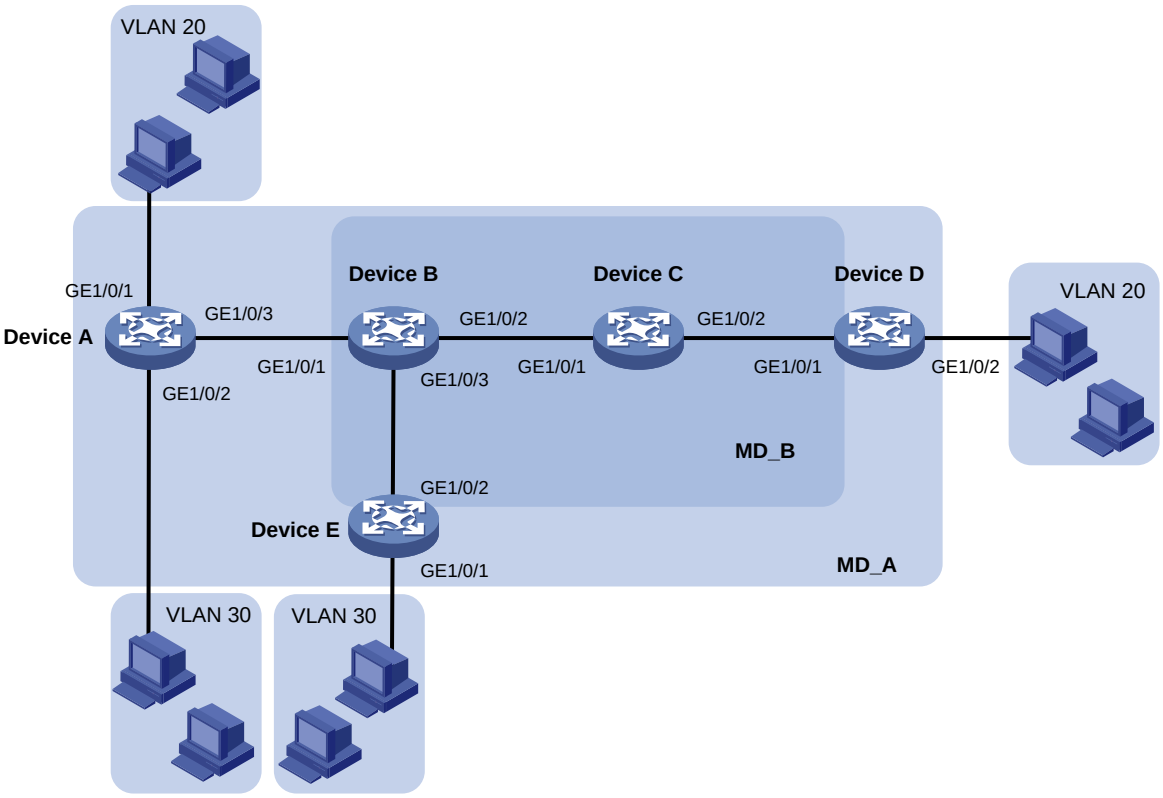
Network configuration

As shown in Figure 1, Device B and Device C reside in the central equipment room of a company. Device A, Device D, and Device E reside in other areas.

- Research and development department users in VLAN 20 access the enterprise network through Device A and Device D.
- Marketing department users in VLAN 30 access the enterprise network through Device A and Device E.

Configure CFD to verify and locate link faults.

Figure 1 Network diagram



Analysis

To accurately locate link faults, assign the enterprise network to MD_A (level 5) and the central equipment room network to MD_B (level 3). MD_A nests MD_B.

To effectively implement CFD, assign MAs based on the VLANs of service traffic:

- Assign VLAN 20 in MD_A to MA_A_1.
- Assign VLAN 30 in MD_A to MA_A_2.
- Assign VLAN 20 in MD_B to MA_B_1.
- Assign VLAN 30 in MD_B to MA_A_2.

To verify link connectivity, configure MEPs on the interfaces located at the boundary of MAs, for example, MA_B_1:

- Configure MEPs on interface GE1/0/1 of Device B and Device D to allow CFD packets from VLAN 20 to pass through the following interfaces:
  - GE1/0/1 and GE1/0/2 of Device B.
  - GE1/0/1 and GE1/0/2 of Device C.
  - GE1/0/1 of Device D.
- Configure GE1/0/1 of Device B as an inward-facing MEP because CFD packets are forwarded through other interfaces on the device.
- Configure GE1/0/1 of Device D as an outward-facing MEP because CFD packets are forwarded through the interface.

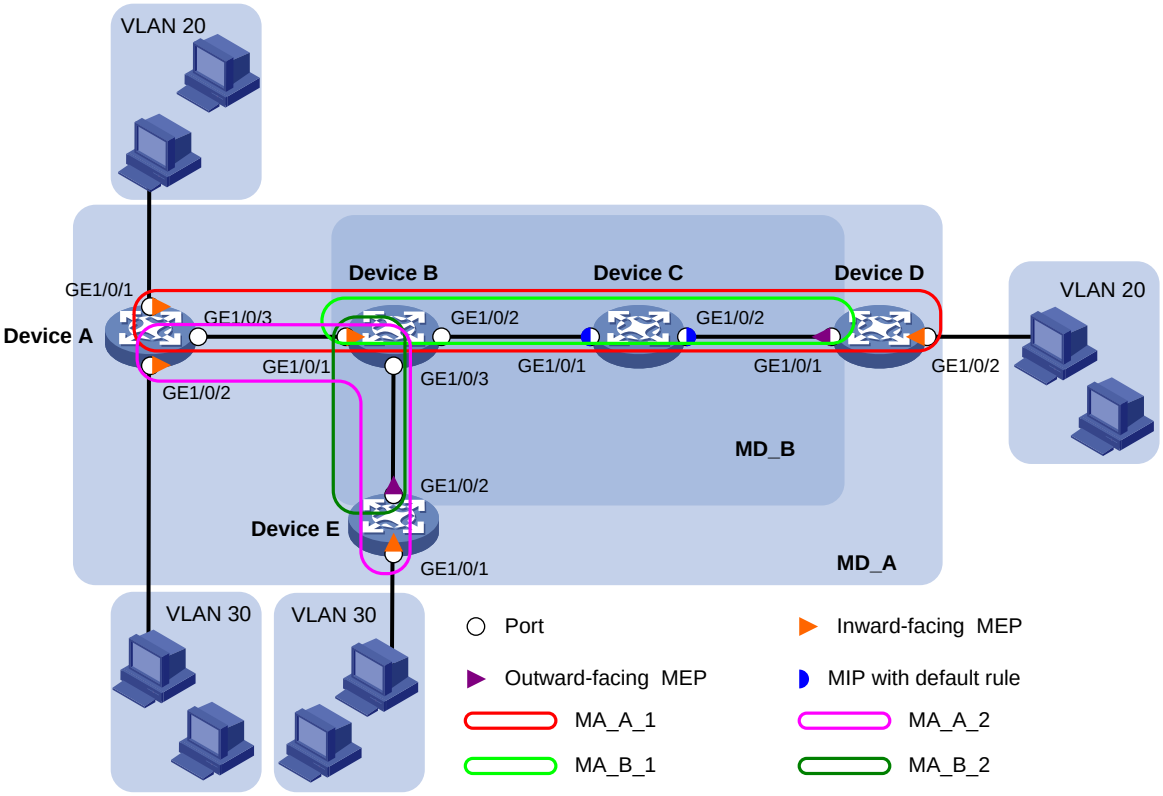
To accurately locate link faults between Device B and Device D, configure the default MIP generation rule on Device C.

To detect connectivity among MEPs, configure CC on the MEPs.

To verify link faults detected through CC, use LB. To trace faulty paths or locate link faults, use LT after the status information of the entire network is obtained.

Figure 2 shows a CFD configuration diagram based on the previous analysis.

Figure 2 CFD configuration diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI, and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx

S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure CFD, follow these restrictions and guidelines:

- You cannot create a MEP if the MEP ID is not included in the MEP list of the service instance.
- You can configure multiple MAs in an MD as needed. An MA serves only one VLAN.
- Configure the same CCM interval field value for all MEPs in the same MA. In this example, the MEPs use the default CCM interval field value.

Procedures

Enabling CFD

Enable CFD on Device A.

```
<DeviceA> system-view
[DeviceA] cfd enable
```

Enable CFD on Device B through Device E. (Details not shown.)

Creating VLANs and assigning interfaces to the VLANs

1. Configure Device A:

```
[DeviceA] vlan 20
[DeviceA-vlan20] quit
```

```
[DeviceA] vlan 30
[DeviceA-vlan30] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 20
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 30
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20 30
[DeviceA-GigabitEthernet1/0/3] quit
```

2. Configure Device B:

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
[DeviceB] vlan 30
[DeviceB-vlan30] quit
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20 30
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 20
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 30
[DeviceB-GigabitEthernet1/0/3] quit
```

3. Configure Device C:

```
[DeviceC] vlan 20
[DeviceC-vlan20] quit
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 20
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 20
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure Device D:

```
[DeviceD] vlan 20
[DeviceD-vlan20] quit
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 20
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] interface gigabitethernet 1/0/2
```

```
[DeviceD-GigabitEthernet1/0/2] port access vlan 20
[DeviceD-GigabitEthernet1/0/2] quit
```

5. Configure Device E:

```
[DeviceE] vlan 30
[DeviceE-vlan30] quit
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] port access vlan 30
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 30
[DeviceE-GigabitEthernet1/0/2] quit
```

Configuring service instances

Based on the MAs to which the MEPs belong, perform the configurations as described in the following table:

Device	MD	MD level	MA	VLAN	Service instance
Device A	MD_A	5	MA_A_1	20	1
			MA_A_2	30	2
Device B	MD_B	3	MA_B_1	20	3
			MA_B_2	30	4
Device C	MD_B	3	MA_B_1	20	3
Device D	MD_A	5	MA_A_1	20	1
	MD_B	3	MA_B_1	20	3
Device E	MD_A	5	MA_A_2	30	2
	MD_B	3	MA_B_2	30	4

1. Configure Device A:

   # Create MD_A (level 5).

   ```
   [DeviceA] cfd md MD_A level 5
   ```

   # Create service instance 1, in which the MA named **MA_A_1** serves VLAN 20.

   ```
   [DeviceA] cfd service-instance 1 ma-id string MA_A_1 md MD_A vlan 20
   ```

   # Create service instance 2, in which the MA named **MA_A_2** serves VLAN 30.

   ```
   [DeviceA] cfd service-instance 2 ma-id string MA_A_2 md MD_A vlan 30
   ```

   Configure Device B through Device E in the same way Device A is configured.

2. Configure Device B:

   ```
   [DeviceB] cfd md MD_B level 3
   [DeviceB] cfd service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
   [DeviceB] cfd service-instance 4 ma-id string MA_B_2 md MD_B vlan 30
   ```

3. Configure Device C:

   ```
   [DeviceC] cfd md MD_B level 3
   [DeviceC] cfd service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
   ```

4. Configure Device D:

   ```
   [DeviceD] cfd md MD_A level 5
   ```

```
[DeviceD] cfd service-instance 1 ma-id string MA_A_1 md MD_A vlan 20
[DeviceD] cfd md MD_B level 3
[DeviceD] cfd service-instance 3 ma-id string MA_B_1 md MD_B vlan 20
```

5. Configure Device E:

```
[DeviceE] cfd md MD_A level 5
[DeviceE] cfd service-instance 2 ma-id string MA_A_2 md MD_A vlan 30
[DeviceE] cfd md MD_B level 3
[DeviceE] cfd service-instance 4 ma-id string MA_B_2 md MD_B vlan 30
```

Configuring MEPs

Assign MEP IDs as described in the following table:

Service instance	Device	Interface	MEP ID	MEP type
1	Device A	GigabitEthernet 1/0/1	1001	Inward-facing MEP
	Device D	GigabitEthernet 1/0/2	1002	Inward-facing MEP
2	Device A	GigabitEthernet 1/0/2	2001	Inward-facing MEP
	Device E	GigabitEthernet 1/0/1	2002	Inward-facing MEP
3	Device B	GigabitEthernet 1/0/1	3001	Inward-facing MEP
	Device D	GigabitEthernet 1/0/1	3002	Outward-facing MEP
4	Device B	GigabitEthernet 1/0/1	4001	Inward-facing MEP
	Device E	GigabitEthernet 1/0/2	4002	Outward-facing MEP

1. Configure Device A:

Configure a MEP list in service instances 1 and 2.

```
[DeviceA] cfd meplist 1001 1002 service-instance 1
[DeviceA] cfd meplist 2001 2002 service-instance 2
```

Create inward-facing MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

Create inward-facing MEP 2001 in service instance 2 on GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] cfd mep 2001 service-instance 2 inbound
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

```
[DeviceB] cfd meplist 3001 3002 service-instance 3
[DeviceB] cfd meplist 4001 4002 service-instance 4
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] cfd mep 3001 service-instance 3 inbound
[DeviceB-GigabitEthernet1/0/1] cfd mep 4001 service-instance 4 inbound
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure Device D:

```
[DeviceD] cfd meplist 1001 1002 service-instance 1
[DeviceD] cfd meplist 3001 3002 service-instance 3
```

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] cfd mep 1002 service-instance 1 inbound
[DeviceD-GigabitEthernet1/0/2] quit
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] cfd mep 3002 service-instance 3 outbound
[DeviceD-GigabitEthernet1/0/1] quit
```

4. Configure Device E:

```
[DeviceE] cfd meplist 2001 2002 service-instance 2
[DeviceE] cfd meplist 4001 4002 service-instance 4
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] cfd mep 2002 service-instance 2 inbound
[DeviceE-GigabitEthernet1/0/1] quit
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] cfd mep 4002 service-instance 4 outbound
[DeviceE-GigabitEthernet1/0/2] quit
```

Configuring a MIP generation rule

Configure the MIP generation rule in service instance 3 on Device C as default.

```
[DeviceC] cfd mip-rule default service-instance 3
```

Configuring CC on MEPs

1. Configure Device A:

   # Enable the sending of CCM frames for MEP 1001 in service instance 1 on GigabitEthernet 1/0/1.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] cfd cc service-instance 1 mep 1001 enable
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

   # Enable the sending of CCM frames for MEP 2001 in service instance 2 on GigabitEthernet 1/0/2.

   ```
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] cfd cc service-instance 2 mep 2001 enable
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

   Configure Device B, Device D, and Device E in the same way Device A is configured.

2. Configure Device B:

   ```
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3001 enable
   [DeviceB-GigabitEthernet1/0/1] cfd cc service-instance 4 mep 4001 enable
   [DeviceB-GigabitEthernet1/0/1] quit
   ```

3. Configure Device D:

   ```
   [DeviceD] interface gigabitethernet 1/0/1
   [DeviceD-GigabitEthernet1/0/1] cfd cc service-instance 3 mep 3002 enable
   [DeviceD-GigabitEthernet1/0/1] quit
   [DeviceD] interface gigabitethernet 1/0/2
   [DeviceD-GigabitEthernet1/0/2] cfd cc service-instance 1 mep 1002 enable
   [DeviceD-GigabitEthernet1/0/2] quit
   ```

4. Configure Device E:

   ```
   [DeviceE] interface gigabitethernet 1/0/1
   [DeviceE-GigabitEthernet1/0/1] cfd cc service-instance 2 mep 2002 enable
   [DeviceE-GigabitEthernet1/0/1] quit
   ```

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] cfd cc service-instance 4 mep 4002 enable
[DeviceE-GigabitEthernet1/0/2] quit
```

Verifying the configuration

In this example, the MAC addresses of Device A through Device E are 0010-FC01-6511, 0010-FC02-6512, 0010-FC03-6513, 0010-FC04-6514, and 0010-FC05-6515, respectively.

1. Verify the configuration when the network is operating correctly:

Display information about remote MEP 1001 in service instance 1 on Device A.

```
[DeviceA] display cfd remote-mep service-instance 1 mep 1001
MEP ID   MAC address      State        Time                  MAC status
1002     0010-fc04-6514   OK           2019/07/26 12:54:52   UP
```

The output shows that the remote MEP is operating correctly.

Enable LB on Device A to verify the status of the link between MEP 1001 and MEP 1002 in service instance 1.

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 1002
Loopback to MEP 1002 with the sequence number start from 1001-43404:
Reply from 0010-fc04-6514: sequence number=1001-43404 Time=5ms
Reply from 0010-fc04-6514: sequence number=1001-43405 Time=5ms
Reply from 0010-fc04-6514: sequence number=1001-43406 Time=5ms
Reply from 0010-fc04-6514: sequence number=1001-43407 Time=5ms
Reply from 0010-fc04-6514: sequence number=1001-43408 Time=5ms
Sent: 5        Received: 5        Lost: 0
```

The output shows that no link fault occurs on the link between MEP 1001 and MEP 1002 in service instance 1.

2. Verify the configuration when a link fault occurs:

Display information about remote MEP 1001 in service instance 1 on Device A.

```
[DeviceA] display cfd remote-mep service-instance 1 mep 1001
MEP ID   MAC address      State        Time                  MAC status
1002     0010-fc04-6514   FAILED       2019/07/26 13:01:52   DOWN
```

The output shows that the remote MEP is operating incorrectly.

Enable LB on Device A to verify the status of the link between MEP 1001 and MEP 1002 in service instance 1.

```
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 1002
Loopback to MEP 1002 with the sequence number start from 1001-43904:
Sent: 5        Received: 0        Lost: 5
```

The output shows that a link fault occurs on the link between MEP 1001 and MEP 1002 in service instance 1.

Identify the path between MEP 3001 and MEP 3002 in service instance 3 on Device B.

```
[DeviceB] cfd linktrace service-instance 3 mep 3001 target-mep 3002
Linktrace to MEP 3002 with the sequence number 3001-43862:
MAC Address              TTL     Last Mac         Relay Action
0010-fc03-6513           63      0010-fc02-6512   MPDB
```

The output shows that MEP 3001 receives only the LTR messages from the MIP. No LTR messages are sent from MEP 3002 (GigabitEthernet 1/0/1 on Device D). The link between Device C and Device D fails, and you do not need to troubleshoot the network outside MD_B.

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 cfd enable
 cfd md MD_A index 1 level 5
 cfd service-instance 1 ma-id string MA_A_1 ma-index 1 md MD_A vlan 20
 cfd meplist 1001 to 1002 service-instance 1
 cfd service-instance 2 ma-id string MA_A_2 ma-index 1 md MD_A vlan 30
 cfd meplist 2001 to 2002 service-instance 2
#
vlan 20
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
 cfd mep 1001 service-instance 1 inbound
 cfd cc service-instance 1 mep 1001 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
 cfd mep 2001 service-instance 2 inbound
 cfd cc service-instance 2 mep 2001 enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20 30
```

- Device B:

```
#
 cfd enable
 cfd md MD_B index 1 level 3
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd meplist 3001 to 3002 service-instance 3
 cfd service-instance 4 ma-id string MA_B_2 ma-index 2 md MD_B vlan 30
 cfd meplist 4001 to 4002 service-instance 4
#
vlan 20
#
vlan 30
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20 30
 cfd mep 3001 service-instance 3 inbound
 cfd cc service-instance 3 mep 3001 enable
 cfd mep 4001 service-instance 4 inbound
 cfd cc service-instance 4 mep 4001 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 30
```

- Device C:

```
#
 cfd enable
 cfd md MD_B index 1 level 3
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd mip-rule default service-instance 3
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
```

- Device D:

```
#
 cfd enable
 cfd md MD_A index 1 level 5
 cfd md MD_B index 2 level 3
 cfd service-instance 1 ma-id string MA_A_1 ma-index 1 md MD_A vlan 20
 cfd meplist 1001 to 1002 service-instance 1
 cfd service-instance 3 ma-id string MA_B_1 ma-index 1 md MD_B vlan 20
 cfd meplist 3001 to 3002 service-instance 3
#
vlan 20
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
 cfd mep 3002 service-instance 3 outbound
 cfd cc service-instance 3 mep 3002 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 cfd mep 1002 service-instance 1 inbound
 cfd cc service-instance 1 mep 1002 enable
```

- Device E:

```
#
 cfd enable
 cfd md MD_A index 1 level 5
 cfd md MD_B index 2 level 3
 cfd service-instance 2 ma-id string MA_A_2 ma-index 1 md MD_A vlan 30
 cfd meplist 2001 to 2002 service-instance 2
 cfd service-instance 4 ma-id string MA_B_2 ma-index 2 md MD_B vlan 30
 cfd meplist 4001 to 4002 service-instance 4
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 30
 cfd mep 2002 service-instance 2 inbound
 cfd cc service-instance 2 mep 2002 enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 30
 cfd mep 4002 service-instance 4 outbound
 cfd cc service-instance 4 mep 4002 enable
```

Contents

Introduction

This document provides DLDP configuration examples.

The Device Link Detection Protocol (DLDP) was developed by HP to detect the status of fiber links or twisted-pair links. When DLDP detects unidirectional links, it can automatically shut down the faulty port to avoid network problems. Alternatively, a user can manually shut down the faulty port.

Configuration restrictions and guidelines

When you configure DLDP, follow these restrictions and guidelines:

- For DLDP to operate correctly, configure the full duplex mode for the interfaces at the two ends of the link, and configure the same speed for the two interfaces.
- For DLDP to operate correctly, enable DLDP on both sides and make sure the following settings are consistent:
  - Interval to send Advertisement packets.
  - DLDP authentication mode.
  - Password.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of DLDP.

Example: Configuring the auto port shutdown mode

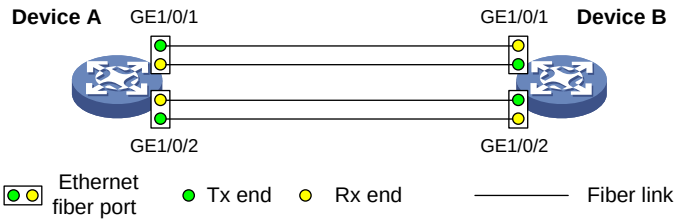
Network configuration

As shown in Figure 1, Device A and Device B are connected through two fiber pairs.

Configure DLDP on the devices so each device performs the following tasks:

- Detects unidirectional links caused by cross-connected fibers or a disconnected fiber.
- Automatically shuts down the faulty interface when detecting a unidirectional link.
- Automatically brings up the interface after the administrator clears the fault.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp global enable
   ```

   # Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to operate in full duplex mode at 1000 Mbps, and enable DLDP on the interfaces.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] duplex full
   [DeviceA-GigabitEthernet1/0/1] speed 1000
   [DeviceA-GigabitEthernet1/0/1] dldp enable
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] duplex full
   [DeviceA-GigabitEthernet1/0/2] speed 1000
   [DeviceA-GigabitEthernet1/0/2] dldp enable
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

   # Set the interval for sending Advertisement packets to 5 seconds (default interval).

   ```
   [DeviceA] dldp interval 5
   ```

   # Configure the plain text authentication mode and set the password to **abc**.

   ```
   [DeviceA] dldp authentication-mode simple
   [DeviceA] dldp authentication-password simple abc
   ```

   # Set the interface shutdown mode to **auto** (default mode).

   ```
   [DeviceA] dldp unidirectional-shutdown auto
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display global and interface-specific DLDP configuration for Device A.

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
```

```
  Neighbor aged time: 11s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
  Neighbor echo time: -
```

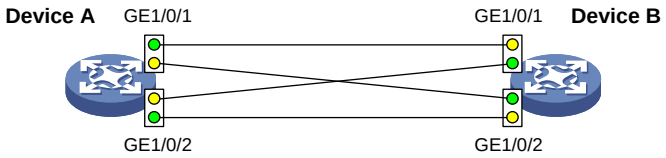
The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is Bidirectional.

Enable the monitoring of logs on the current terminal for Device A, and set the lowest level of the logs that can be output to the monitor terminal to 6.

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

As shown in Figure 2, the two pairs of fibers between Device A and Device B are cross-connected.

Figure 2 Cross-connected fibers



The following log information is displayed on Device A:

```
<DeviceA>%Jul 11 17:40:31:089 2018 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 11 17:40:31:091 2018 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 11 17:40:31:677 2018 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
%Jul 11 17:40:31:678 2018 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 11 17:40:38:544 2018 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to up.
%Jul 11 17:40:38:836 2018 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to up.
```

The output shows that the physical status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is down and then up. The link status of both interfaces is down.

Display information about interface GigabitEthernet 1/0/1 on Device A.

```
[DeviceA]display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: UP
```

```
Line protocol state: DOWN(DLDP)
IP packet frame type: Ethernet II, hardware address: 00e0-fc00-5929
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is optical fiber, Port hardware type is 10G_BASE_SR_SFP
10Gbps-speed mode, full-duplex mode
Link speed type is force link, link duplex type is force link
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
Mdi type: automdix
Port link-type: Access
 Tagged Vlan:   none
 UnTagged Vlan: 1
Port priority: 0
Last link flapping: 0 hours 11 minutes 9 seconds
Last clearing of counters: Never
 Peak input rate: 141 bytes/sec, at 2019-01-01 01:37:08
 Peak output rate: 84 bytes/sec, at 2019-01-01 05:39:56
 Last 300 second input:  0 packets/sec 99 bytes/sec 0%
 Last 300 second output:  0 packets/sec 63 bytes/sec 0%
 Input (total):  26470 packets, 2469445 bytes
          0 unicasts, 1 broadcasts, 26469 multicasts, 0 pauses
 Input (normal):  26470 packets, - bytes
          0 unicasts, 1 broadcasts, 26469 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 16962 packets, 1165236 bytes
          0 unicasts, 0 broadcasts, 16962 multicasts, 0 pauses
 Output (normal): 16962 packets, - bytes
          0 unicasts, 0 broadcasts, 16962 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

The output shows that the physical status of GigabitEthernet 1/0/1 is up, but DLDP automatically shuts down the interface. The output for interface GigabitEthernet 1/0/2 is similar to GigabitEthernet 1/0/1. (Details not shown.)

Display global and interface-specific DLDP configuration for Device A.

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
```

```
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Auto
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is Unidirectional. DLDP has detected a unidirectional link on both interfaces.

Correct the fiber connections. As a result, the ports shut down by DLDP automatically recover, and Device A displays the following log information:

```
<DeviceA>%Jul 11 17:42:57:709 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed to down.
%Jul 11 17:42:58:603 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed to down.
%Jul 11 17:43:02:342 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Jul 11 17:43:02:343 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-3600, and the port index is 1.
%Jul 11 17:43:02:344 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface GigabitEthernet1/0/1.
%Jul 11 17:43:02:353 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1 changed to up.
%Jul 11 17:43:02:357 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Jul 11 17:43:02:362 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-3600, and the port index is 2.
%Jul 11 17:43:02:362 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface GigabitEthernet1/0/2.
%Jul 11 17:43:02:368 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/2 changed to up.
```

The output shows that the physical status and link status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are up and their DLDP neighbors are determined. The links become bidirectional.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 dldp global enable
 dldp authentication-mode simple
 dldp authentication-password cipher $c$3$wHDzwD/AZNW+q+otXapfZ/tUB/Wgbg==
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
```

- The configuration file for Device B is the same as Device A. (Details not shown.)

Example: Configuring the manual port shutdown mode

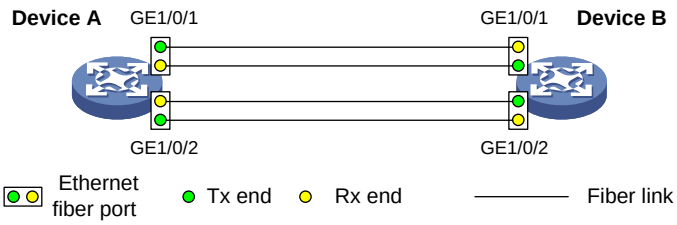
Network configuration

As shown in Figure 3, Device A and Device B are connected through two fiber pairs.

Configure DLDP on the devices to meet the following requirements:

- Each device can detect unidirectional links caused by cross-connected fibers or a disconnected fiber.
- When a unidirectional link is detected, the administrator can manually shut down the faulty port based on the connection status of the link.
- The interface recovers from failure after the administrator clears the fault and manually brings up the port.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

1. Configure Device A:

   # Enable DLDP globally.

   ```
   <DeviceA> system-view
   [DeviceA] dldp global enable
   ```

   # Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to operate in full duplex mode at 1000 Mbps, and enable DLDP on the interfaces.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] duplex full
   [DeviceA-GigabitEthernet1/0/1] speed 1000
   [DeviceA-GigabitEthernet1/0/1] dldp enable
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] duplex full
   [DeviceA-GigabitEthernet1/0/2] speed 1000
   [DeviceA-GigabitEthernet1/0/2] dldp enable
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

   # Set the interval for sending Advertisement packets to 5 seconds (default interval).

   ```
   [DeviceA] dldp interval 5
   ```

   # Configure the plain text authentication mode and set the password to **abc**.

   ```
   [DeviceA] dldp authentication-mode simple
   [DeviceA] dldp authentication-password simple abc
   ```

   # Set the interface shutdown mode to **manual**.

   ```
   [DeviceA] dldp unidirectional-shutdown manual
   ```

2. Configure Device B in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Display global and interface-specific DLDP configuration for Device A.

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
```

```
  Neighbor aged time: 11s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port's neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
  Neighbor echo time: -
```

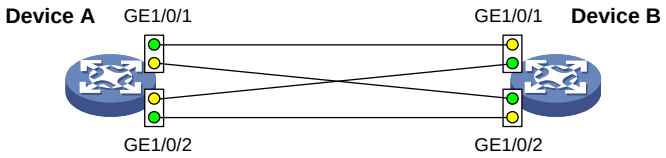
The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is Bidirectional.

Enable the monitoring of logs on the current terminal for Device A, and set the lowest level of the logs that can be output to the monitor terminal to 6.

```
[DeviceA] quit
<DeviceA> terminal monitor
The current terminal is enabled to display logs.
<DeviceA> terminal logging level 6
```

As shown in Figure 4, the two pairs of fibers between Device A and Device B are cross-connected.

Figure 4 Cross-connected fibers



The following log information is displayed on Device A:

```
<DeviceA>%Jul 12 08:29:17:786 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:29:17:787 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:29:17:800 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
%Jul 12 08:29:17:800 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jul 12 08:29:25:004 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to up.
%Jul 12 08:29:25:005 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:29:25:893 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to up.
%Jul 12 08:29:25:894 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
```

The output shows that the physical status and link status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are down and then up.

Display information about interface GigabitEthernet 1/0/1 on Device A.

```
[DeviceA]display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 00e0-fc00-5929
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is optical fiber, Port hardware type is 10G_BASE_SR_SFP
10Gbps-speed mode, full-duplex mode
Link speed type is force link, link duplex type is force link
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
Mdi type: automdix
Port link-type: Access
 Tagged Vlan:   none
 UnTagged Vlan: 1
Port priority: 0
Last link flapping: 0 hours 11 minutes 9 seconds
Last clearing of counters: Never
 Peak input rate: 141 bytes/sec, at 2019-01-01 01:37:08
 Peak output rate: 104 bytes/sec, at 2019-01-01 06:40:58
 Last 300 second input:  0 packets/sec 27 bytes/sec 0%
 Last 300 second output:  1 packets/sec 101 bytes/sec 0%
 Input (total):  27226 packets, 2547709 bytes
          0 unicasts, 1 broadcasts, 27225 multicasts, 0 pauses
 Input (normal):  27226 packets, - bytes
          0 unicasts, 1 broadcasts, 27225 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 17991 packets, 1260564 bytes
          0 unicasts, 0 broadcasts, 17991 multicasts, 0 pauses
 Output (normal): 17991 packets, - bytes
          0 unicasts, 0 broadcasts, 17991 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

The output shows that the physical status and link status of GigabitEthernet 1/0/1 are up. DLDP does not shut down the interface. The output for interface GigabitEthernet 1/0/2 is similar to GigabitEthernet 1/0/1. (Details not shown.)

Display global and interface-specific DLDP configuration for Device A.

```
<DeviceA> display dldp
```

```
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Manual
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port's neighbors: 0 (Maximum number ever detected: 1)
```

The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is Unidirectional. DLDP has detected a unidirectional link on both interfaces but does not shut them down.

Shut down GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:34:23:717 2019 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:34:23:718 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jul 12 08:34:23:778 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
%Jul 12 08:34:23:779 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
```

The output shows that the physical status and link status of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are down.

Shut down GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
```

Correct the fiber connections, and bring up GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-GigabitEthernet1/0/2]%Jul 12 08:46:17:677 2019 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Jul 12 08:46:17:678 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
```

```
%Jul 12 08:46:17:959 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-
3600, and the port index is 2.
%Jul 12 08:46:17:959 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/2.
```

The output shows that the physical status and link status of GigabitEthernet 1/0/2 are up and its DLDP neighbor is determined. The links become bidirectional.

Bring up GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-GigabitEthernet1/0/1]%Jul 12 08:48:25:952 2019 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:48:25:952 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-
3600, and the port index is 1.
%Jul 12 08:48:25:953 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jul 12 08:48:25:953 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/1.
```

The output shows that the physical status and link status of GigabitEthernet 1/0/1 are up and its DLDP neighbor is determined. The links become bidirectional.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 dldp global enable
 dldp authentication-mode simple
 dldp authentication-password cipher $c$3$wHDzwD/AZNW+q+otXapfZ/tUB/Wgbg==
 dldp unidirectional-shutdown manual
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
```

- The configuration file for Device B is the same as Device A. (Details not shown.)

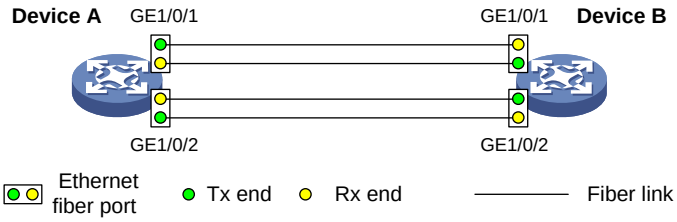
Example: Configuring the hybrid port shutdown mode

Network configuration

As shown in Figure 5, Device A and Device B are connected through two fiber pairs.

Configure DLDP to detect unidirectional links. When a unidirectional link is detected, DLDP automatically shuts down the unidirectional port. The administrator needs to bring up the port after clearing the fault.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx

S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch	Release 63xx

E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

1. Configure Device A:

Enable DLDP globally.

```
<DeviceA> system-view
[DeviceA] dldp enable
```

Configure GigabitEthernet 1/0/1 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] duplex full
[DeviceA-GigabitEthernet1/0/1] speed 1000
[DeviceA-GigabitEthernet1/0/1] dldp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 to operate in full duplex mode and at 1000 Mbps, and enable DLDP on the port.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] duplex full
[DeviceA-GigabitEthernet1/0/2] speed 1000
[DeviceA-GigabitEthernet1/0/2] dldp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Set the interval for sending Advertisement packets to 5 seconds, configure the DLDP authentication mode as **simple**, and configure the password for DLDP authentication as **abc**.

```
[DeviceA] dldp interval 5
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple abc
```

Set the port shutdown mode to **hybrid**.

```
[DeviceA] dldp unidirectional-shutdown hybrid
```

2. Configure Device B in the same way Device A is configured.

Verifying the configuration

Display global and interface-specific DLDP configuration on Device A.

```
[DeviceA] display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Hybrid
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port’s neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 1
  Neighbor state: Confirmed
  Neighbor aged time: 11s
  Neighbor echo time: -

Interface GigabitEthernet1/0/2
 DLDP port state: Bidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 100s
 Number of the port’s neighbors: 1
  Neighbor MAC address: 0023-8956-3600
  Neighbor port index: 2
  Neighbor state: Confirmed
  Neighbor aged time: 12s
  Neighbor echo time: -
```

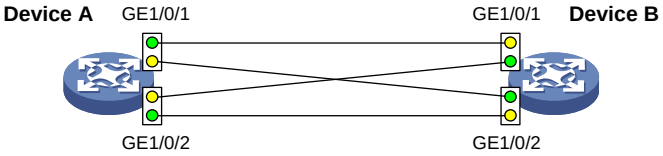
The output shows that both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in bidirectional state, which means both links are bidirectional.

Enable the monitoring of logs on the current terminal on Device A. Set the lowest level of the logs that can be output to the current terminal to 6.

```
[DeviceA] quit
<DeviceA> terminal monitor
<DeviceA> terminal logging level 6
```

As shown in Figure 6, the two pairs of fibers between Device A and Device B are cross-connected..

Figure 6 Cross-connected fibers



The following log information is displayed on Device A:

```
<DeviceA>%Jan  4 07:16:06:556 2019 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on
interface
GigabitEthernet1/0/1 was deleted because the neighbor was aged. The neighbor's system
MAC is 0023-8956-3600, and the port index is 162.
%Jan  4 07:16:06:560 2019 DeviceA DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface
GigabitEthernet1/0/2 was deleted because the neighbor was aged. The neighbor's system
MAC is 0023-8956-3600, and the port index is 165.
%Jan  4 07:16:06:724 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/1 changed to down.
%Jan  4 07:16:06:730 2019 DeviceA IFNET/3/PHY_UPDOWN: Physical state on the interface
GigabitEthernet1/0/2 changed to down.
%Jan  4 07:16:06:736 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Jan  4 07:16:06:738 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Jan  4 07:16:07:152 2019 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a
unidirectional link on interface GigabitEthernet1/0/1. DLDP automatically shut down
the interface. Please manually bring up the interface.
%Jan  4 07:16:07:156 2019 DeviceA DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a
unidirectional link on interface GigabitEthernet1/0/2. DLDP automatically shut down
the interface. Please manually bring up the interface.
```

The output shows that the port status and link status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are down.

Display information about interface GigabitEthernet 1/0/1 on Device A.

```
[DeviceA]display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN(DLDP)
IP packet frame type: Ethernet II, hardware address: 00e0-fc00-5929
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is optical fiber, Port hardware type is 10G_BASE_SR_SFP
10Gbps-speed mode, full-duplex mode
Link speed type is force link, link duplex type is force link
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
```

```
Mdi type: automdix
Port link-type: Access
 Tagged Vlan:   none
 UnTagged Vlan: 1
Port priority: 0
Last link flapping: 0 hours 11 minutes 9 seconds
Last clearing of counters: Never
 Peak input rate: 141 bytes/sec, at 2019-01-01 01:37:08
 Peak output rate: 84 bytes/sec, at 2019-01-01 05:39:56
 Last 300 second input:  0 packets/sec 99 bytes/sec 0%
 Last 300 second output:  0 packets/sec 63 bytes/sec 0%
 Input (total):  26470 packets, 2469445 bytes
          0 unicasts, 1 broadcasts, 26469 multicasts, 0 pauses
 Input (normal):  26470 packets, - bytes
          0 unicasts, 1 broadcasts, 26469 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 16962 packets, 1165236 bytes
          0 unicasts, 0 broadcasts, 16962 multicasts, 0 pauses
 Output (normal): 16962 packets, - bytes
          0 unicasts, 0 broadcasts, 16962 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

The output shows that the physical status and link status of GigabitEthernet 1/0/1 are down. The output for interface GigabitEthernet 1/0/2 is similar to GigabitEthernet 1/0/1. (Details not shown.)

Display global and interface-specific DLDP configuration on Device A.

```
<DeviceA> display dldp
 DLDP global status: Enabled
 DLDP advertisement interval: 5s
 DLDP authentication-mode: Simple
 DLDP authentication-password: ******
 DLDP unidirectional-shutdown mode: Hybrid
 DLDP delaydown-timer value: 1s
 Number of enabled ports: 2

Interface GigabitEthernet1/0/1
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)

Interface GigabitEthernet1/0/2
 DLDP port state: Unidirectional
 DLDP port unidirectional-shutdown mode: None
 DLDP initial-unidirectional-delay: 0s
 Number of the port’s neighbors: 0 (Maximum number ever detected: 1)
```

The output shows that the DLDP port status of both GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 is Unidirectional. DLDP has detected a unidirectional link on both interfaces.

Correct the fiber connections, and bring up GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-GigabitEthernet1/0/1]%Jan  4 07:33:26:574 2019 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Jan  4 07:33:57:562 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/1. The neighbor's system MAC is 0023-8956-
3600, and the port index is 162.
%Jan  4 07:33:57:563 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/1.
%Jan  4 07:33:57:590 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Jan  4 07:33:57:609 2019 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/1 detected a topology change.
```

The output shows that the port status and link status of GigabitEthernet 1/0/1 are now up and its DLDP neighbors are determined. The links become bidirectional.

Bring up GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
```

The following log information is displayed on Device A:

```
[DeviceA-GigabitEthernet1/0/2]%Jan  4 07:35:26:574 2019 DeviceA IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Jan  4 07:35:57:562 2019 DeviceA DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was
confirmed on interface GigabitEthernet1/0/2. The neighbor's system MAC is 0023-8956-
3600, and the port index is 162.
%Jan  4 07:35:57:563 2019 DeviceA DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a
bidirectional link on interface GigabitEthernet1/0/2.
%Jan  4 07:35:57:590 2019 DeviceA IFNET/5/LINK_UPDOWN: Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
%Jan  4 07:35:57:609 2019 DeviceA STP/6/STP_DETECTED_TC: Instance 0's port
GigabitEthernet1/0/2 detected a topology change.
```

The output shows that the port status and link status of GigabitEthernet 1/0/2 are now up and its DLDP neighbors are determined. The links become bidirectional.

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 dldp global enable
 dldp authentication-mode simple
 dldp authentication-password cipher $c$3$wHDzwD/AZNW+q+otXapfZ/tUB/Wgbg==
```

```
 dldp unidirectional-shutdown hybrid
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 speed 1000
 duplex full
 dldp enable
#
```

- The configuration file for Device B is the same as Device A. (Details not shown.)

Contents

Introduction

This document provides VRRP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of VRRP, STP, IPsec, and Ethernet link aggregation.

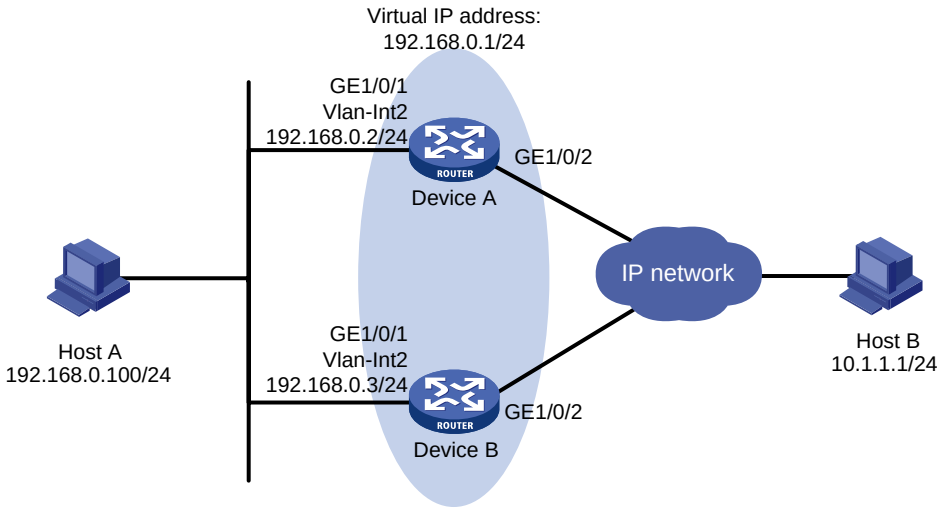
Example: Configuring a single IPv4 VRRP group

Network configuration

As shown in Figure 1, configure a VRRP group on Device A and Device B as the gateway for Host A to meet the following requirements:

- Device A operates as the master to forward packets from Host A to the external network.
- If Device A or its uplink interface fails, Host A can access the external network through Device B.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- For Device A to become the master when it recovers from a failure, configure the preemptive mode for the VRRP group.
- For Device A to decrease its priority and become a backup when its uplink interface fails, configure VRRP tracking on Device A.
- To avoid frequent role change in the VRRP group, set a preemption delay.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI	Release 11xx

Hardware	Software version
and S5500V3-48P-SI)	
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

Hardware	Software version
IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure a single VRRP group, follow these restrictions and guidelines:

- The virtual IP address of a VRRP group cannot be any of the following addresses:
  - All-zero address (0.0.0.0).
  - Broadcast address (255.255.255.255).
  - Loopback address.
  - IP address of other than Class A, Class B, and Class C.
  - Invalid IP address (for example, 0.0.0.1).
- For Host A to access the external network, make sure the following IP addresses are on the same subnet:
  - The virtual IP address of the VRRP group.
  - The downlink interface IP addresses of the VRRP group members.
- IPv4 VRRP can use VRRPv2 or VRRPv3 (default version). For a VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- Removal of the VRRP group on the IP address owner causes IP address collision. To avoid a collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.
- Configure the same virtual IP addresses for each device in the VRRP group.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the VRRP group. Another device in the group can then be elected as the master.

Procedures

Configuring Device A

Create VLAN 2, and assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

Create VLAN-interface 2, and assign an IP address to the VLAN interface.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.2 24
```

Create VRRP group 1, and set its virtual IP address to 192.168.0.1.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.1
```

Set the priority of Device A to 110 in VRRP group 1. Device A has a higher priority than Device B in VRRP group 1, so Device A can become the master.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface2] quit
```

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

Associate VRRP group 1 with track entry 1 to decrease the weight of Device A by 50 when the track entry transits to Negative.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface2] quit
```

Configuring Device B

Create VLAN 2, and assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/1
[DeviceB-vlan2] quit
```

Create VLAN-interface 2, and assign an IP address to the VLAN interface.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.0.3 24
```

Create VRRP group 1, and set its virtual IP address to 192.168.0.1.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.1
```

Set the priority of Device B to 100 in VRRP group 1.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 priority 100
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceB-Vlan-interface2] quit
```

Verifying the configuration

1. Verify that Host A can ping Host B. (Details not shown.)
2. Verify that Device A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

   # Display detailed information about VRRP group 1 on Device A.

```
[DeviceA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
```

```
    Auth Type      : None
    Virtual IP     : 192.168.0.1
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 192.168.0.2
  VRRP Track Information:
    Track Object   : 1                  State : Positive   Pri Reduced : 50
```

Display detailed information about VRRP group 1 on Device B.

```
[DeviceB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Become Master  : 401ms left
     Auth Type      : None
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
```

3. Disconnect the link between Host A and Device A, and verify that Host A can still ping Host B. (Details not shown.)

4. Verify that Device B takes over to forward packets from Host A to Host B when Device A fails.

```
[DeviceB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.3
```

5. Verify that Device A becomes the master to forward packets from Host A to Host B after Device A recovers.

```
[DeviceA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 110                Running Pri  : 110
     Preempt Mode   : Yes                Delay Time   : 500
```

```
    Auth Type      : None
    Virtual IP     : 192.168.0.1
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 192.168.0.2
  VRRP Track Information:
    Track Object   : 1                  State : Positive   Pri Reduced : 50
```

Configuration files

NOTE:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 50
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 track 1 interface GigabitEthernet1/0/2
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 100
 vrrp vrid 1 preempt-mode delay 500
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
```

#

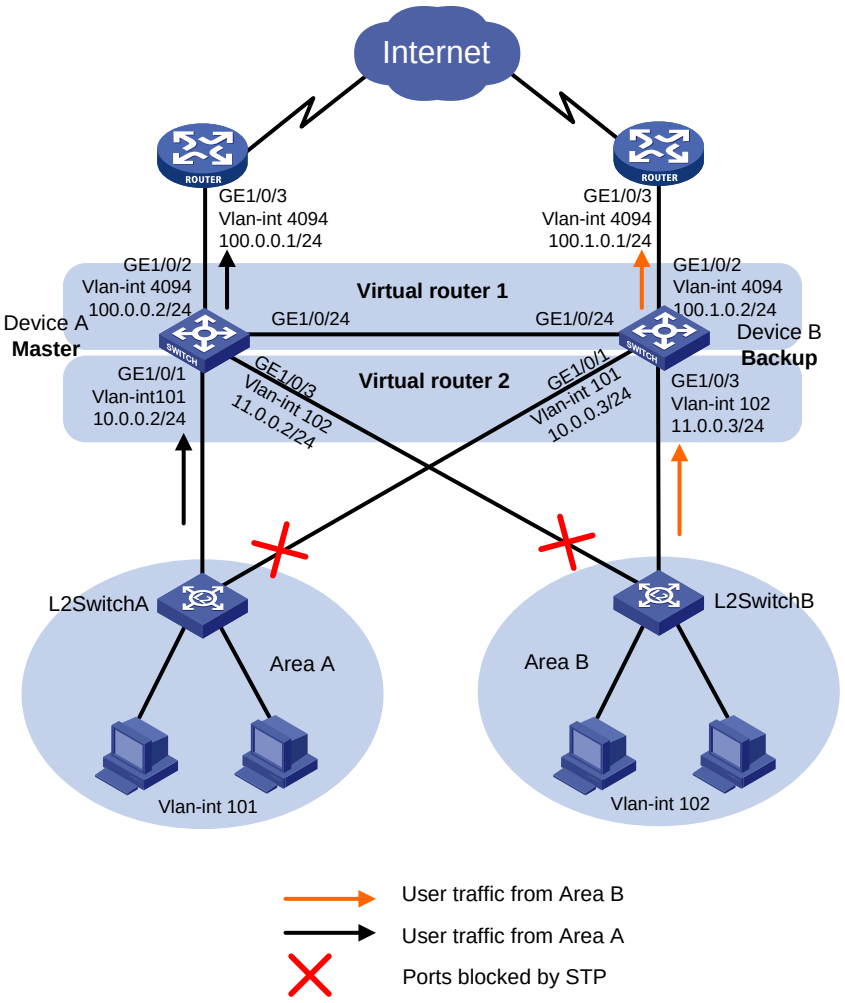
Example: Configuring multiple IPv4 VRRP groups

Network configuration

As shown in Figure 2, configure two VRRP groups on Device A and Device B as gateways for internal hosts to meet the following requirements:

- Device A operates as the master of VRRP group 1 to forward packets from Area A, and Device B operates as the master of VRRP group 2 to forward packets from Area B. When one of the devices fails, the other device provides gateway service for both areas.
- If the uplink interface of one device fails, hosts can access the external network through the other device.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To avoid frequent role change in the VRRP group, set a preemption delay.
- To avoid loops between Device A, Device B, and the Layer 2 switches, use the spanning tree feature to block a port in the two VRRP groups.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

Hardware	Software version
S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported

Hardware	Software version
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure multiple VRRP groups, follow these restrictions and guidelines:

- The virtual IP address of a VRRP group cannot be any of the following addresses:
  - All-zero address (0.0.0.0).
  - Broadcast address (255.255.255.255).
  - Loopback address.
  - IP address of other than Class A, Class B, and Class C.
  - Invalid IP address (for example, 0.0.0.1).
- For the hosts in both areas to access the external network, make sure the following IP addresses for each VRRP group are on the same subnet:
  - The virtual IP address of the VRRP group.
  - The downlink interface IP addresses of the VRRP group members.
- IPv4 VRRP can use VRRPv2 or VRRPv3 (default version). For a VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- Removal of the VRRP group on the IP address owner causes IP address collision. To avoid a collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the VRRP group. Another device in the group can then be elected as the master.
- Make sure the following configurations are the same on the members of a VRRP group:
  - Number of virtual IP addresses.
  - Virtual IP addresses.
  - Advertisement interval.

Procedures

Configuring Device A

Create VLAN 101, and assign GigabitEthernet 1/0/1 to VLAN 101.

```
<DeviceA> system-view
[DeviceA] vlan 101
[DeviceA-vlan101] port gigabitethernet 1/0/1
[DeviceA-vlan101] quit
```

Create VLAN-interface 101, and assign an IP address to the VLAN interface.

```
[DeviceA] interface vlan-interface 101
```

```
[DeviceA-Vlan-interface101] ip address 10.0.0.2 24
[DeviceA-Vlan-interface101] quit
```

Assign IP addresses to other VLAN interfaces of Device A. (Details not shown.)

Configure GigabitEthernet 1/0/24 as a trunk port, and assign it to VLAN 101 and VLAN 102.

```
[DeviceA] interface gigabitethernet 1/0/24
[DeviceA-GigabitEthernet1/0/24] port link-type trunk
[DeviceA-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/24] port trunk permit vlan 101 to 102
[DeviceA-GigabitEthernet1/0/24] port trunk pvid vlan 101
[DeviceA-GigabitEthernet1/0/24] quit
```

Disable the spanning tree feature on GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create VRRP group 1, and set its virtual IP address to 10.0.0.1. Assign Device A a higher priority than Device B in VRRP group 1, so Device A can become the master.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 1 virtual-ip 10.0.0.1
```

Set the priority of Device A to 120 in VRRP group 1. Device A has a higher priority than Device B in VRRP group 1, so Device A can become the master.

```
[DeviceA-Vlan-interface101] vrrp vrid 1 priority 120
[DeviceA-Vlan-interface101] quit
```

Create VRRP group 2, and set its virtual IP address to 11.0.0.1.

```
[DeviceA] interface vlan-interface 102
[DeviceA-Vlan-interface102] vrrp vrid 2 virtual-ip 11.0.0.1
[DeviceA-Vlan-interface102] quit
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface101] quit
```

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

Associate VRRP group 1 with track entry 1 to decrease the weight of Device A by 50 when the track entry transits to Negative.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface101] quit
```

Configure MSTP, map VLAN 101 to MSTI 1 and VLAN 102 to MSTI 2, and configure Device A as the root bridge of MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name vrrp
[DeviceA-mst-region] instance 1 vlan 101
[DeviceA-mst-region] instance 2 vlan 102
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
[DeviceA] stp instance 1 root primary
```

```
[DeviceA] stp instance 2 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create VLAN 101, and assign GigabitEthernet 1/0/1 to VLAN 101.

```
<DeviceB> system-view
[DeviceB] vlan 101
[DeviceB-vlan101] port gigabitethernet 1/0/1
[DeviceB-vlan101] quit
```

Create VLAN-interface 101, and assign an IP address to the VLAN interface.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] ip address 10.0.0.3 24
[DeviceB-Vlan-interface101] quit
```

Assign IP addresses to other VLAN interfaces of Device B. (Details not shown.)

Configure GigabitEthernet 1/0/24 as a trunk port, and assign it to VLAN 101 and VLAN 102.

```
[DeviceB] interface gigabitethernet 1/0/24
[DeviceB-GigabitEthernet1/0/24] port link-type trunk
[DeviceB-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/24] port trunk permit vlan 101 to 102
[DeviceB-GigabitEthernet1/0/24] port trunk pvid vlan 101
[DeviceB-GigabitEthernet1/0/24] quit
```

Disable the spanning tree feature on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create VRRP group 1, and set its virtual IP address to 10.0.0.1.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 1 virtual-ip 10.0.0.1
[DeviceB-Vlan-interface101] quit
```

Create VRRP group 2, and set its virtual IP address to 11.0.0.1. Assign Device B a higher priority than Device A in VRRP group 2, so Device B can become the master.

```
[DeviceB] interface vlan-interface 102
[DeviceB-Vlan-interface102] vrrp vrid 2 virtual-ip 11.0.0.1
```

Set the priority of Device B to 120 in VRRP group 2. Device B has a higher priority than Device A in VRRP group 2, so Device B can become the master.

```
[DeviceB-Vlan-interface102] vrrp vrid 2 priority 120
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface102] vrrp vrid 2 preempt-mode delay 500
[DeviceB-Vlan-interface102] quit
```

Create track entry 2 to monitor the link status of the uplink interface GigabitEthernet 1/0/2.

```
[DeviceB] track 2 interface gigabitethernet 1/0/2
[DeviceB-track-2] quit
```

Associate VRRP group 2 with track entry 2 to decrease the weight of Device A by 50 when the track entry transits to Negative.

```
[DeviceB] interface vlan-interface 102
[DeviceB-Vlan-interface102] vrrp vrid 2 track 2 priority reduced 50
[DeviceB-Vlan-interface102] quit
```

Configure MSTP, map VLAN 101 to MSTI 1 and VLAN 102 to MSTI 2, and configure Device B as the root bridge of MSTI 2.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name vrrp
[DeviceB-mst-region] instance 1 vlan 101
[DeviceB-mst-region] instance 2 vlan 102
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
[DeviceB] stp instance 2 root primary
[DeviceB] stp instance 1 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring L2SwitchA

Set the MST region name of the device to **vrrp**.

```
<L2SwitchA> system-view
[L2SwitchA] stp region-configuration
[L2SwitchA-mst-region] region-name vrrp
```

Map VLAN 101 to MSTI 1 and activate the MST region configuration

```
[L2SwitchA-mst-region] instance 1 vlan 101
[L2SwitchA-mst-region] active region-configuration
[L2SwitchA-mst-region] quit
```

Enable the spanning tree feature globally.

```
[L2SwitchA] stp global enable
```

Configuring L2SwitchB

Set the MST region name of the device to **vrrp**.

```
<L2SwitchB> system-view
[L2SwitchB] stp region-configuration
[L2SwitchB-mst-region] region-name vrrp
```

Map VLAN 102 to MSTI 1 and activate the MST region configuration.

```
[L2SwitchB-mst-region] instance 1 vlan 102
[L2SwitchB-mst-region] active region-configuration
[L2SwitchB-mst-region] quit
```

Enable the spanning tree feature globally.

```
[L2SwitchB] stp global enable
```

Verifying the configuration

1. Verify that the hosts in Area A and Area B can ping the external network.

   # Ping 100.0.0.1 from Host A in Area A.

   ```
   <host A> ping 100.0.0.1
   ```

```
PING 100.0.0.1 (100.0.0.1): 56 data bytes
56 bytes from 100.0.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.0.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.0.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.0.0.1: seq=3 ttl=128 time=7.45 ms
56 bytes from 100.0.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

Ping 100.1.0.1 from Host C in Area B.

```
<host C> ping 100.1.0.1
PING 100.1.0.1 (100.1.0.1): 56 data bytes
56 bytes from 100.1.0.1: seq=0 ttl=128 time=22.43 ms
56 bytes from 100.1.0.1: seq=1 ttl=128 time=7.17 ms
56 bytes from 100.1.0.1: seq=2 ttl=128 time=8.91 ms
56 bytes from 100.1.0.1: seq=3 ttl=128 time=7.45 ms
56 bytes from 100.1.0.1: seq=4 ttl=128 time=9.11 ms

--- 100.1.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

2. Verify that Device A is operating as the master in VRRP group 1 and the backup in VRRP group 2. Device B is operating as the backup in VRRP group 1 and the master in VRRP group 2.

Display detailed information about the VRRP groups on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID            : 1                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 120               Running Pri  : 120
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.0.0.1
     Virtual MAC     : 0000-5e00-0101
     Master IP       : 10.0.0.2
   VRRP Track Information:
     Track Object    : 1                 State : Positive   Pri Reduced : 50

   Interface Vlan-interface102
     VRID            : 2                 Adver Timer  : 100
     Admin Status    : Up                State        : Backup
     Config Pri      : 100               Running Pri  : 100
     Preempt Mode    : Yes               Delay Time   : 0
     Auth Type       : None
```

```
    Virtual IP     : 11.0.0.1
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 11.0.0.3
```

Display detailed information about the VRRP groups on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 10.0.0.2

   Interface Vlan-interface102
     VRID           : 2                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 120               Running Pri  : 120
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 11.0.0.1
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 11.0.0.3
   VRRP Track Information:
     Track Object   : 2                 State : Positive   Pri Reduced : 50
```

3. Verify that Device B becomes the master in VRRP group 1 when Device A fails.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.0.0.3

   Interface Vlan-interface102
     VRID           : 2                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 120               Running Pri  : 120
```

```
    Preempt Mode   : Yes                Delay Time   : 500
    Auth Type      : None
    Virtual IP     : 11.0.0.1
    Virtual MAC    : 0000-5e00-0102
    Master IP      : 11.0.0.3
  VRRP Track Information:
    Track Object   : 2                  State : Positive   Pri Reduced : 50
```

4. Verify that Device A becomes the master in VRRP group 1 after it recovers.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 120                Running Pri  : 120
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.0.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.0.0.2
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50

   Interface Vlan-interface102
     VRID           : 2                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 0
     Become Master  : 3550ms left
     Auth Type      : None
     Virtual IP     : 11.0.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 11.0.0.3
```

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 101 to 102
#
vlan 4094
#
stp region-configuration
 region-name vrrp
```

```
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
stp instance 1 root primary
stp instance 2 root secondary
 stp global enable
#
interface Vlan-interface101
 ip address 10.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 50
#
interface Vlan-interface102
 ip address 11.0.0.2 255.255.255.0
 vrrp vrid 2 virtual-ip 11.0.0.1
#
interface Vlan-interface4094
 ip address 100.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 102
#
interface GigabitEthernet1/0/24
port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
 track 1 interface GigabitEthernet1/0/2
#
```

- Device B:

```
#
vlan 101 to 102
#
```

```
vlan 4094
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
stp instance 2 root primary
stp instance 1 root secondary
 stp global enable
#
interface Vlan-interface101
 ip address 10.0.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.0.0.1
#
interface Vlan-interface102
 ip address 11.0.0.3 255.255.255.0
 vrrp vrid 2 virtual-ip 11.0.0.1
 vrrp vrid 2 priority 120
vrrp vrid 2 preempt-mode delay 500
vrrp vrid 2 track 2 priority reduced 50
#
interface Vlan-interface4094
 ip address 100.1.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 102
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
 track 2 interface GigabitEthernet1/0/2
#
```

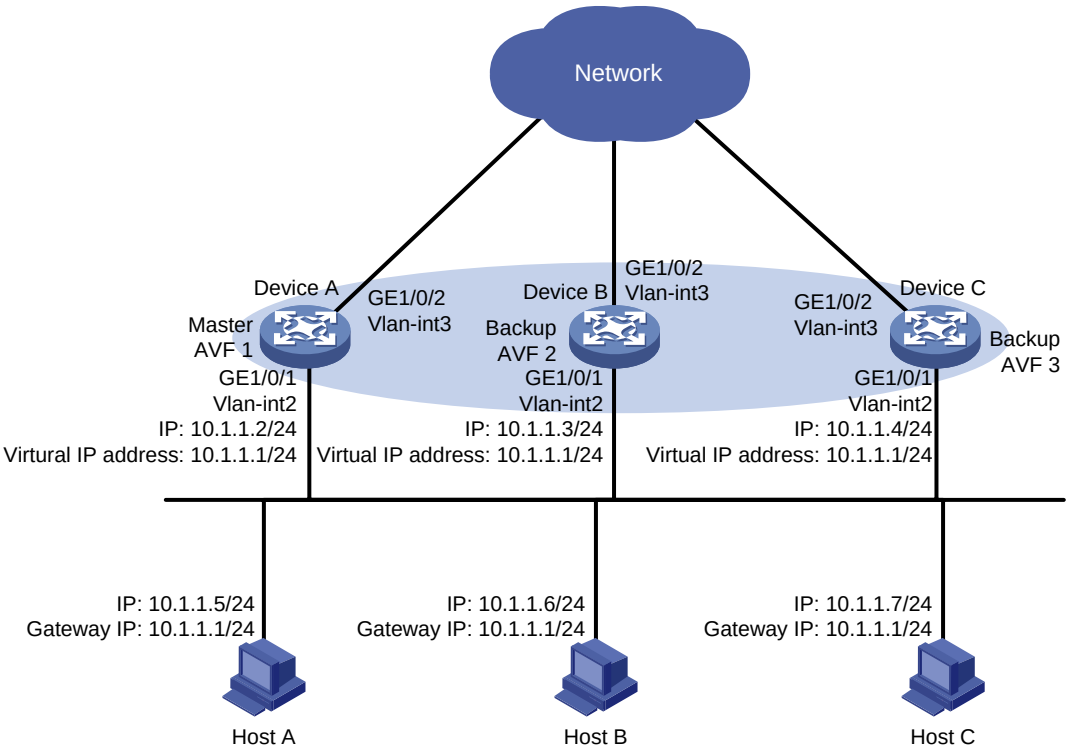
Example: Configuring IPv4 VRRP load balancing

Network configuration

As shown in Figure 3, configure a load-balanced VRRP group on Device A, Device B, and Device C as the gateway for the hosts to meet the following requirements:

- Packets from the hosts are load balanced among the devices.
- If one device fails, hosts can access the external network through the other devices.

Figure 3 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To avoid frequent role change in the VRRP group, set a preemption delay.
- For traffic to be switched to the other two devices when the uplink interface of one device fails, configure VF tracking on Device A, Device B, and Device C. When the uplink interface of one device fails, the weights of the VFs (including the AVF) on the device decrease by the specified value.
- For the failed device to become the master when it recovers, configure the preemptive mode for the VRRP group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure VRRP load balancing, follow these restrictions and guidelines:

- The virtual IP address of a VRRP group cannot be any of the following addresses:
  - All-zero address (0.0.0.0).
  - Broadcast address (255.255.255.255).
  - Loopback address.
  - IP address of other than Class A, Class B, and Class C.
  - Invalid IP address (for example, 0.0.0.1).
- For the hosts to access the external network, make sure the following IP addresses are on the same subnet:
  - The virtual IP address of the VRRP group.
  - The downlink interface IP addresses of the VRRP group members.
- IPv4 VRRP can use VRRPv2 or VRRPv3 (default version). For a VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- In load balancing mode, the virtual IP address of a VRRP group cannot be the IP address of any interface in the VRRP group. Otherwise, VRRP load balancing cannot operate correctly.
- If the uplink interface of the VF owner fails, an LVF must take over as the AVF. The switchover occurs when the weight of the VF owner drops below the lower limit of failure. This requires the reduced weight for the VF owner to be higher than 245.
- Configure the same virtual IP addresses for each device in the VRRP group.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the VRRP group. Another device in the group can then be elected as the master.

Procedures

Configuring Device A

1. Configure the interfaces:

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.2 24
[DeviceA-Vlan-interface2] quit
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] quit
```

2. Configure VRRP:

Configure VRRP to operate in load balancing mode.

```
[DeviceA] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[DeviceA] interface vlan-interface 2
```

```
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Set the priority of Device A to 120 in VRRP group 1. Device A has the highest priority in VRRP group 1, so Device A can become the master.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 priority 120
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2. If the uplink interface fails, the track entry transits to Negative.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 weight track 1 weight reduced 250
[DeviceA-Vlan-interface2] quit
```

Configuring Device B

1. Configure the interfaces:

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/1
[DeviceB-vlan2] quit
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 10.1.1.3 24
[DeviceB-Vlan-interface2] quit
[DeviceB] vlan 3
[DeviceB-vlan3] port gigabitethernet 1/0/2
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] quit
```

2. Configure VRRP:

Configure VRRP to operate in load balancing mode.

```
[DeviceB] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Set the priority of Device B to 110 in VRRP group 1. Device B has a higher priority than Device C in VRRP group 1, so Device B can become the master when Device A fails.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceB-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet3 /0/2. When the uplink interface fails, the track entry transits to Negative.

```
[DeviceB] track 1 interface gigabitethernet 1/0/2
[DeviceB-track-1] quit
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp vrid 1 weight track 1 weight reduced 250
[DeviceB-Vlan-interface2] quit
```

Configuring Device C

1. Configure the interfaces:

```
<DeviceC> system-view
[DeviceC] vlan 2
[DeviceC-vlan2] port gigabitethernet 1/0/1
[DeviceC-vlan2] quit
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ip address 10.1.1.4 24
[DeviceC-Vlan-interface2] quit
[DeviceC] vlan 3
[DeviceC-vlan3] port gigabitethernet 1/0/2
[DeviceC-vlan3] quit
[DeviceC] interface vlan-interface 3
[DeviceC-Vlan-interface3] quit
```

2. Configure VRRP:

Configure VRRP to operate in load balancing mode.

```
[DeviceC] vrrp mode load-balance
```

Create VRRP group 1, and set its virtual IP address to 10.1.1.1.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
```

Configure Device C to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceC-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceC-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2. When the uplink interface fails, the track entry transits to Negative.

```
[DeviceC] track 1 interface gigabitethernet 1/0/2
[DeviceC-track-1] quit
```

Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] vrrp vrid 1 weight track 1 weight reduced 250
[DeviceC-Vlan-interface2] quit
```

Verifying the configuration

1. Verify that Host A can ping the external network. (Details not shown.)
2. Verify that Device A is operating as the master and Device B and Device C as the backups in VRRP group 1. Each of the three devices has one AVF and two LVFs.

   # Display detailed information about VRRP group 1 on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Master
     Config Pri     : 120                 Running Pri  : 120
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : 10.1.1.4
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

   # Display detailed information about VRRP group 1 on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
```

```
  Interface Vlan-interface2
    VRID           : 1                    Adver Timer  : 100
    Admin Status   : Up                   State        : Backup
    Config Pri     : 110                  Running Pri  : 110
    Preempt Mode   : Yes                  Delay Time   : 500
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.3 (Local, Backup)
                     10.1.1.2 (Master)
                     10.1.1.4 (Backup)
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Listening
    Virtual MAC    : 000f-e2ff-0011 (Learnt)
    Owner ID       : 0000-5e01-1101
    Priority       : 127
    Active         : 10.1.1.2
   Forwarder 02
    State          : Active
    Virtual MAC    : 000f-e2ff-0012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Device C.

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Backup
     Config Pri     : 100                  Running Pri  : 100
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
```

```
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Listening
    Virtual MAC    : 000f-e2ff-0011 (Learnt)
    Owner ID       : 0000-5e01-1101
    Priority       : 127
    Active         : 10.1.1.2
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : 10.1.1.3
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

3. Verify that AVF switchover can be performed when the uplink interface of Device A fails.

Display detailed information about VRRP group 1 on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.2 (Local, Master)
                      10.1.1.3 (Backup)
                      10.1.1.4 (Backup)
   Forwarder Information: 3 Forwarders 0 Active
     Config Weight  : 255
     Running Weight : 5
   Forwarder 01
     State          : Initialize
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 0
     Active         : 10.1.1.4
```

```
    Forwarder 02
      State          : Initialize
      Virtual MAC    : 000f-e2ff-0012 (Learnt)
      Owner ID       : 0000-5e01-1103
      Priority       : 0
      Active         : 10.1.1.3
    Forwarder 03
      State          : Initialize
      Virtual MAC    : 000f-e2ff-0013 (Learnt)
      Owner ID       : 0000-5e01-1105
      Priority       : 0
      Active         : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object   : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about VRRP group 1 on Device C.

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
      State          : Active
      Virtual MAC    : 000f-e2ff-0011 (Take Over)
      Owner ID       : 0000-5e01-1101
      Priority       : 85
      Active         : local
      Redirect Time  : 93 secs
      Time-out Time  : 1293 secs
    Forwarder 02
      State          : Listening
      Virtual MAC    : 000f-e2ff-0012 (Learnt)
      Owner ID       : 0000-5e01-1103
      Priority       : 85
      Active         : 10.1.1.3
    Forwarder 03
```

```
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that when the uplink interface of Device A fails, the weights of the VFs on Device A drop below the lower limit of failure. All VFs on Device A transit to Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Device C becomes the AVF to forward traffic.

4. Verify that the VF for virtual MAC address 000f-e2ff-0011 is removed from Device C when the timeout timer (about 1800 seconds) expires. The VF no longer forwards the packets destined for the MAC address.

```
[DeviceC] display vrrp verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : 10.1.1.1
     Member IP List : 10.1.1.4 (Local, Backup)
                      10.1.1.2 (Master)
                      10.1.1.3 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : 10.1.1.3
    Forwarder 03
     State          : Active
     Virtual MAC    : 000f-e2ff-0013 (Owner)
     Owner ID       : 0000-5e01-1105
     Priority       : 255
     Active         : local
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

5. Verify that Device B has a higher priority than Device C and becomes the master when Device A fails.

```
[DeviceB] display vrrp verbose
```

```
IPv4 Standby Information:
    Run mode : Load balance
    Run Method     : Virtual MAC
Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1                   Adver Timer  : 1
    Admin Status   : Up                  State        : Master
    Config Pri     : 110                 Running Pri  : 110
    Preempt Mode   : Yes                 Delay Time   : 500
    Auth Type      : None
    Virtual IP     : 10.1.1.1
    Member IP List : 10.1.1.3 (Local, Master)
                     10.1.1.4 (Backup)
  Forwarder Information: 2 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 02
    State          : Active
    Virtual MAC    : 000f-e2ff-0012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : 10.1.1.4
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 weight track 1 weight reduced 250
```

```
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface GigabitEthernet1/0/2
#
```

- Device B:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 weight track 1 weight reduced 250
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface GigabitEthernet1/0/2
#
```

- Device C:

```
#
 vrrp mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.4 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 500
```

```
 vrrp vrid 1 weight track 1 weight reduced 250
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface GigabitEthernet1/0/2
#
```

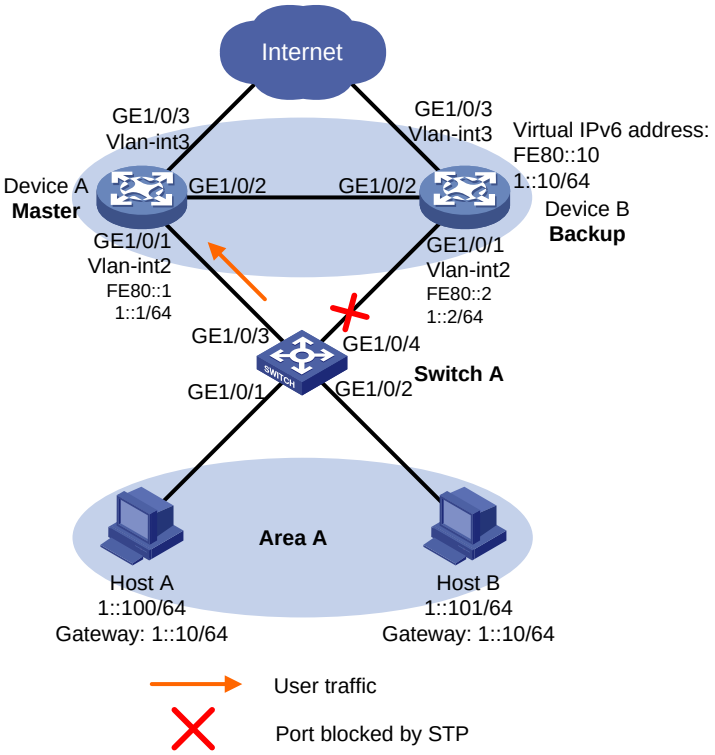
Example: Configuring a single IPv6 VRRP group

Network configuration

As shown in Figure 4, configure an IPv6 VRRP group on Device A and Device B as the gateway for hosts in Area A to meet the following requirements:

- Device A operates as the master to forward packets from the hosts in Area A to the external network.
- If Device A or its uplink interface fails, the hosts in Area A can access the external network through Device B.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- For Device A to become the master when it recovers from a failure, configure the preemptive mode for the VRRP group.
- For Device A to decrease its priority and become a backup when its uplink interface fails, configure VRRP tracking on Device A.
- To avoid frequent role change in the VRRP group, set a preemption delay.
- To avoid loops between Device A, Device B, and the Layer 2 switches, use the spanning tree feature to block a port in the IPv6 VRRP group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx

Hardware	Software version
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

Hardware	Software version
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure a single IPv6 VRRP group, follow these restrictions and guidelines:

- For the hosts in Area A to access the external network, make sure the following IP addresses are on the same subnet:
  - The virtual IPv6 address of the VRRP group.
  - The downlink interface IPv6 addresses of the VRRP group members.
- IPv6 VRRP can use VRRPv2 or VRRPv3 (default version). For an IPv6 VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.

- Removal of the IPv6 VRRP group on the IP address owner causes IP address collision. To avoid a collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.
- Configure the same virtual IPv6 addresses for each device in the IPv6 VRRP group.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the IPv6 VRRP group. Another device in the group can then be elected as the master.

Procedures

Configuring Device A

Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

Create VLAN-interface 2 and assign IPv6 addresses to the VLAN interface.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ipv6 address fe80::1 link-local
[DeviceA-Vlan-interface2] ipv6 address 1::1 64
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Disable RA message suppression on VLAN-interface 2. The hosts in Area A can learn the default gateway address from the RA messages.

```
[DeviceA-Vlan-interface2] undo ipv6 nd ra halt
```

Set the priority of Device A to 110 in IPv6 VRRP group 1. Device A has a higher priority than Device B in IPv6 VRRP group 1, so Device A can become the master.

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface2] quit
```

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/3.

```
[DeviceA] track 1 interface gigabitethernet 1/0/3
[DeviceA-track-1] quit
```

Associate IPv6 VRRP group 1 with track entry 1 and decrease the device priority by 50 when the state of track entry 1 changes to Negative.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface2] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLAN 2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/2] port trunk pvid vlan 2
```

```
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure MSTP, map VLAN 2 to MSTI 1, and configure Device A as the root bridge of MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name vrrp
[DeviceA-mst-region] instance 1 vlan 2
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
[DeviceA] stp instance 1 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/1
[DeviceB-vlan2] quit
```

Create VLAN-interface 2 and assign IPv6 addresses to the VLAN interface.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ipv6 address fe80::2 link-local
[DeviceB-Vlan-interface2] ipv6 address 1::2 64
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Disable RA message suppression on VLAN-interface 2. The hosts in Area A can learn the default gateway address from the RA messages.

```
[DeviceB-Vlan-interface2] undo ipv6 nd ra halt
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 500
[DeviceB-Vlan-interface2] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLAN 2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2
[DeviceB-GigabitEthernet1/0/2] port trunk pvid vlan 2
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure MSTP, map VLAN 2 to MSTI 1, and configure Device B as a secondary root bridge in MSTI 1.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name vrrp
[DeviceB-mst-region] instance 1 vlan 2
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
[DeviceB] stp instance 1 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring Switch A

Set the MST region name of the device to **vrrp**.

```
<SwitchA> system-view
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
```

Map VLAN 2 to MSTI 1 and activate the MST region configuration.

```
[SwitchA-mst-region] instance 1 vlan 2
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
```

Enable the spanning tree feature globally.

```
[SwitchA] stp global enable
```

Verifying the configuration

1. Verify that Host A in Area A can ping the IPv6 address 30::1.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that Device A is operating as the master and Device B as the backup in IPv6 VRRP group 1. Device A forwards packets from the hosts in Area A to the external network.

Display detailed information about IPv6 VRRP group 1 on Device A.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
```

```
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::1
  VRRP Track Information:
    Track Object   : 1                  State : Positive   Pri Reduced : 50
```

Display detailed information about IPv6 VRRP group 1 on Device B.

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Become Master  : 3000ms left
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
```

3. Verify that Host A can still ping the IPv6 address 30::1 after Device A or its uplink interface fails.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

4. Verify that Device B takes over to forward packets from the hosts in Area A to the external network after Device A or its uplink interface fails.

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
```

```
    Auth Type      : None
    Virtual IP     : FE80::10
                     1::10
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::2
```

5. Verify that Device A becomes the master to forward packets from the hosts in Area A to the external network when Device A or its uplink interface recovers.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 50
```

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp instance 1 root primary
 stp global enable
#
interface Vlan-interface2
ipv6 address fe80::1 link-local
ipv6 address 1::1/64
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
```

```
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 #
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2
 port trunk pvid vlan 2
#
 track 1 interface GigabitEthernet1/0/3
#
```

- Device B:

```
#
 sysname DeviceB
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp instance 1 root secondary
 stp global enable
#
interface Vlan-interface2
 ipv6 address fe80::2 link-local
ipv6 address 1::2/64
 undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode delay 500
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2
 port trunk pvid vlan 2
#
```

- Switch A:

```
#
 sysname SwitchA
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp global enable
#
```

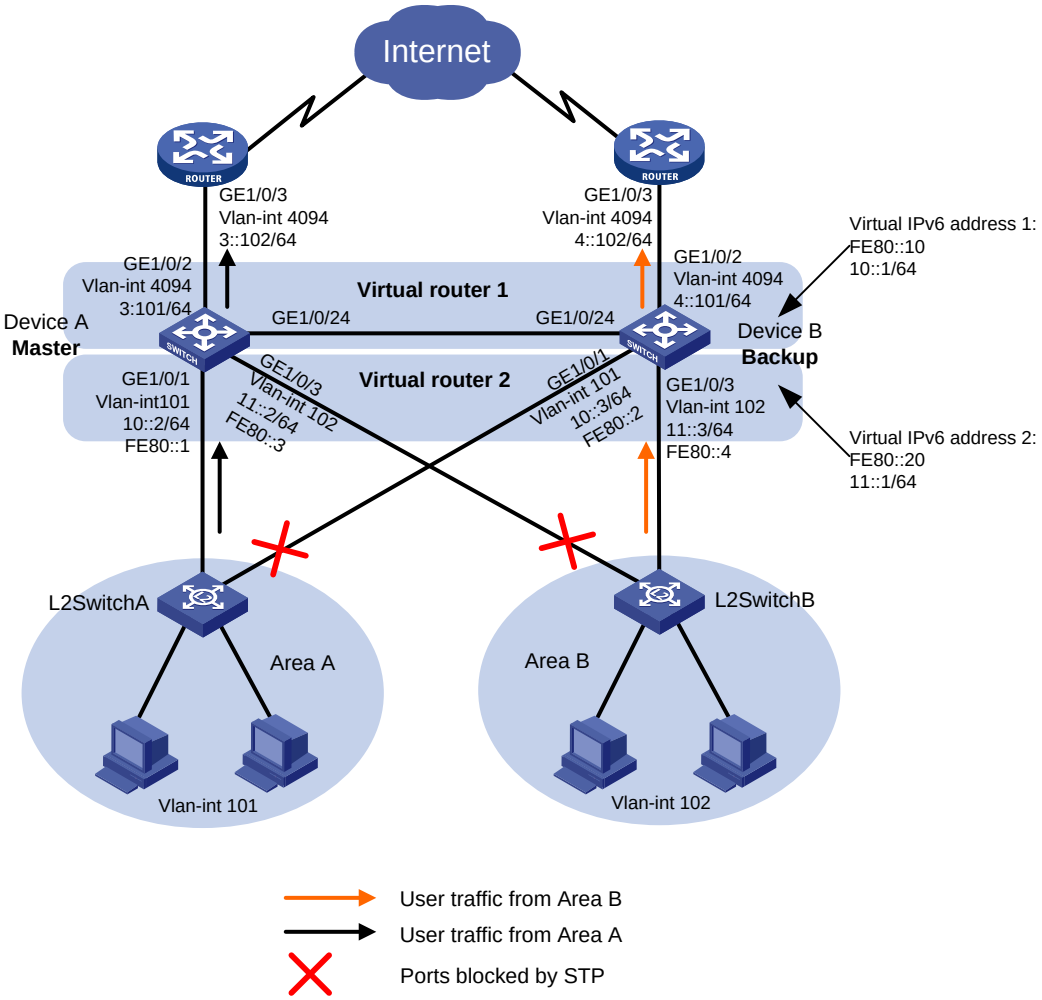
Example: Configuring multiple IPv6 VRRP groups

Network configuration

As shown in Figure 5, configure two IPv6 VRRP groups on Device A and Device B as gateways for internal hosts to meet the following requirements:

- Device A operates as the master of IPv6 VRRP group 1 to forward packets from Area A. Device B operates as the master of IPv6 VRRP group 2 to forward packets from Area B.
- When one device or its uplink interface fails, the other device provides gateway service for both areas.

Figure 5 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To avoid frequent role change in the VRRP group, set a preemption delay.
- For Device A or Device B to decrease its priority and become a backup in an IPv6 VRRP group when the uplink interface of the device fails, configure VRRP tracking on both devices.
- To avoid loops between Device A, Device B, and the Layer 2 switches, use the spanning tree feature to block a port in each IPv6 VRRP group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI	Not supported

Hardware	Software version
S5120V3-54P-PWR-SI	
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure multiple IPv6 VRRP groups, follow these restrictions and guidelines:

- For the hosts in both areas to access the external network, make sure the following IP addresses for each VRRP group are on the same subnet:
  - The virtual IPv6 address of the VRRP group.

    - The downlink interface IPv6 addresses of the VRRP group members.
- IPv6 VRRP can use VRRPv2 or VRRPv3 (default version). For an IPv6 VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- Removal of the IPv6 VRRP group on the IP address owner causes IP address collision. To avoid a collision, change the IPv6 address of the interface on the IP address owner before you remove the VRRP group from the interface.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the VRRP group. Another device in the group can then be elected as the master.
- Make sure the following configurations are the same on the members of an IPv6 VRRP group:
    - Number of virtual IPv6 addresses.
    - Virtual IPv6 addresses.
    - Advertisement interval.

Procedures

Configuring Device A

Create VLAN 101 and assign GigabitEthernet 1/0/1 to VLAN 101.

```
<DeviceA> system-view
[DeviceA] vlan 101
[DeviceA-vlan101] port gigabitethernet 1/0/1
[DeviceA-vlan101] quit
```

Create VLAN-interface 101, and assign IPv6 addresses to VLAN-interface 101.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ipv6 address fe80::1 link-local
[DeviceA-Vlan-interface101] ipv6 address 10::2 64
[DeviceA-Vlan-interface101] quit
```

Assign IPv6 addresses to other VLAN interfaces of Device A. (Details not shown.)

Configure GigabitEthernet 1/0/24 as a trunk port and assign the port to VLAN 101 and VLAN 102.

```
[DeviceA] interface gigabitethernet 1/0/24
[DeviceA-GigabitEthernet1/0/24] port link-type trunk
[DeviceA-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/24] port trunk permit vlan 101 to 102
[DeviceA-GigabitEthernet1/0/24] port trunk pvid vlan 101
[DeviceA-GigabitEthernet1/0/24] quit
```

Disable the spanning tree feature on GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 10::1.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 10::1
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface101] vrrp ipv6 vrid 1 preempt-mode delay 500
```

Set the priority of Device A to 120 in IPv6 VRRP group 1. Device A has a higher priority than Device B in IPv6 VRRP group 1, so Device A can become the master.

```
[DeviceA-Vlan-interface101] vrrp ipv6 vrid 1 priority 120
```

Disable RA message suppression on VLAN-interface 101. The hosts in Area A can learn the default gateway address from the RA messages.

```
[DeviceA-Vlan-interface101] undo ipv6 nd ra halt
[DeviceA-Vlan-interface101] quit
```

Create IPv6 VRRP group 2, and set its virtual IPv6 addresses to FE80::20 and 11::1.

```
[DeviceA] interface vlan-interface 102
[DeviceA-Vlan-interface102] vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
[DeviceA-Vlan-interface102] vrrp ipv6 vrid 2 virtual-ip 11::1
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface102] vrrp ipv6 vrid 2 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 102. The hosts in Area B can learn the default gateway address from the RA messages.

```
[DeviceA-Vlan-interface102] undo ipv6 nd ra halt
[DeviceA-Vlan-interface102] quit
```

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

Associate IPv6 VRRP group 1 with track entry 1 and decrease the device priority by 50 when the state of track entry 1 changes to Negative.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp ipv6 vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface101] quit
```

Configure MSTP, map VLAN 101 to MSTI 1 and VLAN 102 to MSTI 2, and configure Device A as the root bridge of MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name vrrp
[DeviceA-mst-region] instance 1 vlan 101
[DeviceA-mst-region] instance 2 vlan 102
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
[DeviceA] stp instance 1 root primary
[DeviceA] stp instance 2 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create VLAN 101, and assign GigabitEthernet 1/0/1 to VLAN 101.

```
<DeviceB> system-view
[DeviceB] vlan 101
[DeviceB-vlan101] port gigabitethernet 1/0/1
[DeviceB-vlan101] quit
```

Create VLAN-interface 101, and assign IPv6 addresses to VLAN-interface 101.

```
[DeviceB] interface vlan-interface 101
```

```
[DeviceB-Vlan-interface101] ipv6 address fe80::2 link-local
[DeviceB-Vlan-interface101] ipv6 address 10::3 64
[DeviceB-Vlan-interface101] quit
```

Assign IPv6 addresses to other VLAN interfaces of Device B. (Details not shown.)

Configure GigabitEthernet 1/0/24 as a trunk port, and assign the port to VLAN 101 and VLAN 102.

```
[DeviceB] interface gigabitethernet 1/0/24
[DeviceB-GigabitEthernet1/0/24] port link-type trunk
[DeviceB-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/24] port trunk permit vlan 101 to 102
[DeviceB-GigabitEthernet1/0/24] port trunk pvid vlan 101
[DeviceB-GigabitEthernet1/0/24] quit
```

Disable the spanning tree feature on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 10::1.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-Vlan-interface101] vrrp ipv6 vrid 1 virtual-ip 10::1
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface101] vrrp ipv6 vrid 1 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 101. The hosts in Area A can learn the default gateway address from the RA messages.

```
[DeviceB-Vlan-interface101] undo ipv6 nd ra halt
[DeviceB-Vlan-interface101] quit
```

Create IPv6 VRRP group 2, and set its virtual IPv6 addresses to FE80::20 and 11::1.

```
[DeviceB] interface vlan-interface 102
[DeviceB-Vlan-interface102] vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
[DeviceB-Vlan-interface102] vrrp ipv6 vrid 2 virtual-ip 11::1
```

Set the priority of Device B to 120 in IPv6 VRRP group 2. Device B has a higher priority than Device A in IPv6 VRRP group 2, so Device B can become the master.

```
[DeviceB-Vlan-interface102] vrrp ipv6 vrid 2 priority 120
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface102] vrrp ipv6 vrid 2 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 102. The hosts in Area B can learn the default gateway address from the RA messages.

```
[DeviceB-Vlan-interface102] undo ipv6 nd ra halt
[DeviceB-Vlan-interface102] quit
```

Create track entry 2 to monitor the link status of the uplink interface GigabitEthernet 1/0/2.

```
[DeviceB] track 2 interface gigabitethernet 1/0/2
[DeviceB-track-2] quit
```

Associate IPv6 VRRP group 2 with track entry 2 and decrease the device priority by 50 when the state of track entry 2 changes to Negative.

```
[DeviceB] interface vlan-interface 102
[DeviceB-Vlan-interface102] vrrp ipv6 vrid 2 track 2 priority reduced 50
```

```
[DeviceB-Vlan-interface102] quit
```

Configure MSTP, map VLAN 101 to MSTI 1 and VLAN 102 to MSTI 2, and configure Device B as the root bridge of MSTI 2.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name vrrp
[DeviceB-mst-region] instance 1 vlan 101
[DeviceB-mst-region] instance 2 vlan 102
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
[DeviceB] stp instance 2 root primary
[DeviceB] stp instance 1 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring L2SwitchA

Set the MST region name of the device to **vrrp**.

```
<L2SwitchA> system-view
[L2SwitchA] stp region-configuration
[L2SwitchA-mst-region] region-name vrrp
```

Map VLAN 101 to MSTI 1, and activate the MST region configuration.

```
[L2SwitchA-mst-region] instance 1 vlan 101
[L2SwitchA-mst-region] active region-configuration
[L2SwitchA-mst-region] quit
```

Enable the spanning tree feature globally.

```
[L2SwitchA] stp global enable
```

Configuring L2SwitchB

Set the MST region name of the device to **vrrp**.

```
<L2SwitchB> system-view
[L2SwitchB] stp region-configuration
[L2SwitchB-mst-region] region-name vrrp
```

Map VLAN 102 to MSTI 1, and activate the MST region configuration.

```
[L2SwitchB-mst-region] instance 1 vlan 102
[L2SwitchB-mst-region] active region-configuration
[L2SwitchB-mst-region] quit
```

Enable the spanning tree feature globally.

```
[L2SwitchB] stp global enable
```

Verifying the configuration

1. Verify that the hosts in both Area A and Area B can ping the external network.

   # Ping the IPv6 address 30::1 from a host in Area A.

   ```
   Microsoft Windows [Version 6.1.7601]
   Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
   ```

```
C:\Users\areaA>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping the IPv6 address 30::1 from a host in Area B.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\areaB>ping 30::1

Pinging 30::1 with 32 bytes of data:
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms
Reply from 30::1: time<1ms

Ping statistics for 30::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that Device A is operating as the master in IPv6 VRRP group 1 and the backup in IPv6 VRRP group 2. Device B is operating as the master in IPv6 VRRP group 2 and the backup in IPv6 VRRP group 1.

Display detailed information about all IPv6 VRRP groups on Device A.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 120               Running Pri  : 120
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      10::1
     Virtual MAC    : 0000-5e00-0201
     Master IP      : FE80::1
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 50
```

```
  Interface Vlan-interface102
    VRID            : 2                   Adver Timer  : 100
    Admin Status    : Up                  State        : Backup
    Config Pri      : 100                 Running Pri  : 100
    Preempt Mode    : Yes                 Delay Time   : 500
    Auth Type       : None
    Become Master   : 3550ms left
    Virtual MAC     : 0000-5e00-0201
    Virtual IP      : FE80::20
                      11::1
    Master IP       : FE80::4
```

Display detailed information about all IPv6 VRRP groups on Device B.

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
     VRID            : 1                   Adver Timer  : 100
     Admin Status    : Up                  State        : Backup
     Config Pri      : 100                 Running Pri  : 100
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Become Master   : 3500ms left
     Virtual IP      : FE80::10
                       10::2
     Virtual MAC     : 0000-5e00-0202
     Master IP       : FE80::1

   Interface Vlan-interface102
     VRID            : 2                   Adver Timer  : 100
     Admin Status    : Up                  State        : Master
     Config Pri      : 120                 Running Pri  : 120
     Preempt Mode    : Yes                 Delay Time   : 500
     Auth Type       : None
     Virtual IP      : FE80::20
                       11::1
     Virtual MAC     : 0000-5e00-0202
     Master IP       : FE80::4
   VRRP Track Information:
     Track Object    : 2                 State : Positive   Pri Reduced : 50
```

3. Verify that Device B becomes the master in IPv6 VRRP group 1 when Device A or its uplink interface fails.

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
```

```
    VRID            : 1                 Adver Timer  : 100
    Admin Status    : Up                State        : Master
    Config Pri      : 100               Running Pri  : 100
    Preempt Mode    : Yes               Delay Time   : 500
    Auth Type       : None
    Virtual IP      : FE80::10
                      10::2
    Virtual MAC     : 0000-5e00-0101
    Master IP       : FE80::2

  Interface Vlan-interface102
    VRID            : 2                 Adver Timer  : 100
    Admin Status    : Up                State        : Master
    Config Pri      : 120               Running Pri  : 120
    Preempt Mode    : Yes               Delay Time   : 500
    Auth Type       : None
    Virtual IP      : FE80::20
                      11::1
    Virtual MAC     : 0000-5e00-0202
    Master IP       : FE80::4
   VRRP Track Information:
    Track Object    : 2                 State : Positive   Pri Reduced : 50
```

4. Verify that Device A becomes the master in IPv6 VRRP group 1 after Device A or its uplink interface recovers.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface101
    VRID            : 1                 Adver Timer  : 100
    Admin Status    : Up                State        : Master
    Config Pri      : 120               Running Pri  : 120
    Preempt Mode    : Yes               Delay Time   : 500
    Auth Type       : None
    Virtual IP      : FE80::10
                      10::1
    Virtual MAC     : 0000-5e00-0201
    Master IP       : FE80::1
   VRRP Track Information:
    Track Object    : 1                 State : Positive   Pri Reduced : 50

   Interface Vlan-interface102
    VRID            : 2                 Adver Timer  : 100
    Admin Status    : Up                State        : Backup
    Config Pri      : 100               Running Pri  : 100
    Preempt Mode    : Yes               Delay Time   : 500
    Auth Type       : None
    Become Master   : 3550ms left
    Virtual IP      : FE80::20
```

```
                  11::1
    Virtual MAC    : 0000-5e00-0201
    Master IP      : FE80::4
```

Configuration files

NOTE:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 101 to 102
#
vlan 4094
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
stp instance 1 root primary
stp instance 2 root secondary
 stp global enable
#
interface Vlan-interface101
ipv6 address fe80::1 link-local
ipv6 address 10::2/64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 10::1
vrrp ipv6 vrid 1 priority 120
vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 track 1 priority reduced 50
#
interface Vlan-interface102
 ipv6 address fe80::3 link-local
ipv6 address 11::2/64
undo ipv6 nd ra halt
vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 11::1
vrrp ipv6 vrid 2 preempt-mode delay 500
#
interface Vlan-interface4094
ipv6 address 3::101/64
undo stp enable
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 102
#
interface GigabitEthernet1/0/24
port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
 track 1 interface GigabitEthernet1/0/2
#
```

- Device B:

```
#
vlan 101 to 102
#
vlan 4094
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 instance 2 vlan 102
 active region-configuration
#
stp instance 2 root primary
stp instance 1 root secondary
 stp global enable
#
interface Vlan-interface101
ipv6 address fe80::3 link-local
ipv6 address 10::3/64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 10::1
vrrp ipv6 vrid 1 preempt-mode delay 500
#
interface Vlan-interface102
ipv6 address fe80::2 link-local
ipv6 address 11::3/64
```

```
undo ipv6 nd ra halt
 vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
 vrrp ipv6 vrid 2 virtual-ip 11::1
vrrp ipv6 vrid 2 priority 120
vrrp ipv6 vrid 2 preempt-mode delay 500
 vrrp ipv6 vrid 2 track 2 priority reduced 50
#
interface Vlan-interface4094
ipv6 address 4::101/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 102
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 101 to 102
 port trunk pvid vlan 101
#
 track 2 interface GigabitEthernet1/0/2
#
```

- L2Switch A:

```
#
 sysname L2SwitchA
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 101
 active region-configuration
#
 stp global enable
#
```

- L2Switch B:

```
#
 sysname L2SwitchB
#
stp region-configuration
```

```
 region-name vrrp
 instance 1 vlan 102
 active region-configuration
#
 stp global enable
#
```

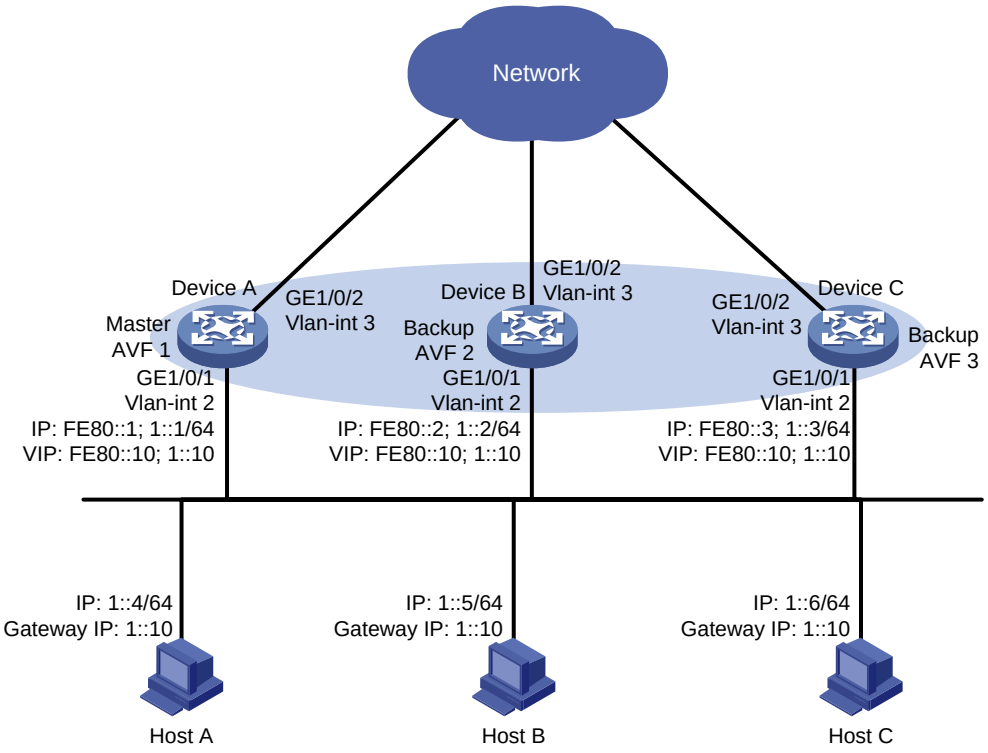
Example: Configuring IPv6 VRRP load balancing

Network configuration

As shown in Figure 6, configure a load-balanced VRRP group on Device A, Device B, and Device C as the gateway for the hosts to meet the following requirements:

- Packets from the hosts are load balanced among the devices.
- If one device fails, hosts can access the external network through the other devices.

Figure 6 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To avoid frequent role change in the VRRP group, set a preemption delay.
- For traffic to be switched to the other two devices when the uplink interface of one device fails, configure VF tracking on Device A, Device B, and Device C. When the uplink interface of one

device fails, the weights of the VFs (including the AVF) on the device decrease by the specified value.

- For the failed device to become the master when it recovers, configure the preemptive mode for the VRRP group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx

Hardware	Software version
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series	Release 63xx

Hardware	Software version
IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure IPv6 VRRP load balancing, follow these restrictions and guidelines:

- For the hosts to access the external network, make sure the following IP addresses are on the same subnet:
  - The virtual IPv6 address of the VRRP group.
  - The downlink interface IPv6 addresses of the VRRP group members.
- IPv6 VRRP can use VRRPv2 or VRRPv3 (default version). For an IPv6 VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- In load balancing mode, the virtual IPv6 addresses of a VRRP group cannot be the IPv6 addresses of any interfaces in the VRRP group. Otherwise, VRRP load balancing cannot operate correctly.
- If the uplink of the VF owner fails, an LVF must take over as the AVF. The switchover occurs when the weight of the VF owner drops below the lower limit of failure. This requires the reduced weight for the VF owner to be higher than 245.
- Configure the same virtual IPv6 addresses for each device in the IPv6 VRRP group.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the IPv6 VRRP group. Another device in the group can then be elected as the master.

Procedures

Configuring Device A

1. Configure the interfaces:

   # Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

   ```
   <DeviceA> system-view
   [DeviceA] vlan 2
   [DeviceA-vlan2] port gigabitethernet 1/0/1
   [DeviceA-vlan2] quit
   ```

   # Create VLAN-interface 2, and assign IPv6 addresses to the VLAN interface.

   ```
   [DeviceA] interface vlan-interface 2
   [DeviceA-Vlan-interface2] ipv6 address fe80::1 link-local
   [DeviceA-Vlan-interface2] ipv6 address 1::1 64
   [DeviceA-Vlan-interface2] quit
   ```

2. Configure VRRP:

   # Configure IPv6 VRRP to operate in load balancing mode.

   ```
   [DeviceA] vrrp ipv6 mode load-balance
   ```

   # Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

   ```
   [DeviceA] interface vlan-interface 2
   ```

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Set the priority of Device A to 120 in IPv6 VRRP group 1. Device A has the highest priority in the VRRP group, so Device A can become the master.

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 priority 120
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 2. The hosts on subnet 1::/64 can learn the default gateway address from the RA messages.

```
[DeviceA-Vlan-interface2] undo ipv6 nd ra halt
[DeviceA-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2. If the uplink interface fails, the track entry transits to Negative.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

Configure the VFs in IPv6 VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
[DeviceA-Vlan-interface2] quit
```

Configuring Device B

1. Configure the interfaces:

Create VLAN 2 and assign Ten-GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-vlan2] port gigabitethernet 1/0/1
[DeviceB-vlan2] quit
```

Create VLAN-interface 2, and assign IPv6 addresses to the VLAN interface.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ipv6 address fe80::2 link-local
[DeviceB-Vlan-interface2] ipv6 address 1::2 64
[DeviceB-Vlan-interface2] quit
```

2. Configure VRRP:

Configure IPv6 VRRP to operate in load balancing mode.

```
[DeviceB] vrrp ipv6 mode load-balance
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Set the priority of Device B to 110 in IPv6 VRRP group 1. Device B has a higher priority than Device C in the VRRP group, so Device B can become the master when Device A fails.

```
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 2. The hosts on subnet 1::/64 can learn the default gateway address from the RA messages.

```
[DeviceB-Vlan-interface2] undo ipv6 nd ra halt
[DeviceB-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2. If the uplink interface fails, the track entry transits to Negative.

```
[DeviceB] track 1 interface gigabitethernet 1/0/2
[DeviceB-track-1] quit
```

Configure the VFs in IPv6 VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
[DeviceB-Vlan-interface2] quit
```

Configuring Device C

1. Configure the interfaces:

Create VLAN 2 and assign Ten-GigabitEthernet 1/0/1 to VLAN 2.

```
<DeviceC> system-view
[DeviceC] vlan 2
[DeviceC-vlan2] port gigabitethernet 1/0/1
[DeviceC-vlan2] quit
```

Create VLAN-interface 2, and assign IPv6 addresses to the VLAN interface.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ipv6 address fe80::3 link-local
[DeviceC-Vlan-interface2] ipv6 address 1::3 64
[DeviceC-Vlan-interface2] quit
```

2. Configure VRRP:

Configure VRRP to operate in load balancing mode.

```
[DeviceC] vrrp ipv6 mode load-balance
```

Create IPv6 VRRP group 1, and set its virtual IPv6 addresses to FE80::10 and 1::10.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[DeviceC-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Configure Device C to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceC-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode delay 500
```

Disable RA message suppression on VLAN-interface 2. The hosts on subnet 1::/64 can learn the default gateway address from the RA messages.

```
[DeviceC-Vlan-interface2] undo ipv6 nd ra halt
[DeviceC-Vlan-interface2] quit
```

3. Configure Track:

Create track entry 1 to monitor the link status of the uplink interface GigabitEthernet 1/0/2. If the uplink interface fails, the track entry transits to Negative.

```
[DeviceC] track 1 interface gigabitethernet 1/0/2
[DeviceC-track-1] quit
```

Configure the VFs in IPv6 VRRP group 1 to monitor track entry 1, and decrease their weights by 250 when the track entry transits to Negative.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] vrrp ipv6 vrid 1 weight track 1 reduced 250
[DeviceC-Vlan-interface2] quit
```

Verifying the configuration

1. Verify that Host A can ping the external network. (Details not shown.)
2. Verify that Device A is operating as the master and Device B and Device C as the backups in IPv6 VRRP group 1. Each of the three devices has one AVF and two LVFs.

   # Display detailed information about all IPv6 VRRP groups on Device A.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer  : 100
     Admin Status   : Up                   State        : Master
     Config Pri     : 120                  Running Pri  : 120
     Preempt Mode   : Yes                  Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
                      FE80::2 (Backup)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Owner)
     Owner ID       : 0000-5e01-1101
     Priority       : 255
     Active         : local
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
     Priority       : 127
     Active         : FE80::2
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
```

```
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about all IPv6 VRRP groups on Device B.

```
[DeviceB] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 110                 Running Pri  : 110
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::2 (Local, Backup)
                      FE80::1 (Master)
                      FE80::3 (Backup)
   Forwarder Information: 3 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Listening
     Virtual MAC    : 000f-e2ff-0011 (Learnt)
     Owner ID       : 0000-5e01-1101
     Priority       : 127
     Active         : FE80::1
    Forwarder 02
     State          : Active
     Virtual MAC    : 000f-e2ff-0012 (Owner)
     Owner ID       : 0000-5e01-1103
     Priority       : 255
     Active         : local
    Forwarder 03
     State          : Listening
     Virtual MAC    : 000f-e2ff-0013 (Learnt)
     Owner ID       : 0000-5e01-1105
     Priority       : 127
     Active         : FE80::3
   Forwarder Weight Track Information:
     Track Object   : 1          State : Positive   Weight Reduced : 250
```

Display detailed information about all VRRP groups on Device C.

```
[DeviceC] display vrrp ipv6 verbose
IPv4 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
```

```
    Admin Status   : Up                  State        : Backup
    Config Pri     : 100                 Running Pri  : 100
    Preempt Mode   : Yes                 Delay Time   : 500
    Auth Type      : None
  Virtual IP     : FE80::10
                   1::10
    Member IP List : FE80::3 (Local, Backup)
                   FE80::1 (Master)
                   FE80::2 (Backup)
  Forwarder Information: 3 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 01
    State          : Listening
    Virtual MAC    : 000f-e2ff-0011 (Learnt)
    Owner ID       : 0000-5e01-1101
    Priority       : 127
    Active         : FE80::1
   Forwarder 02
    State          : Listening
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 127
    Active         : FE80::2
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

3. Verify that AVF switchover can be performed when the uplink interface Ten-GigabitEthernet 1/0/2 of Device A fails.

Display detailed information about all IPv6 VRRP groups on Device A.

```
[DeviceA] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 120               Running Pri  : 120
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : None
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::1 (Local, Master)
```

```
                    FE80::2 (Backup)
                    FE80::3 (Backup)
  Forwarder Information: 3 Forwarders 0 Active
    Config Weight  : 255
    Running Weight : 5
   Forwarder 01
    State          : Initialize
    Virtual MAC    : 000f-e2ff-0011 (Owner)
    Owner ID       : 0000-5e01-1101
    Priority       : 0
    Active         : FE80::3
   Forwarder 02
    State          : Initialize
    Virtual MAC    : 000f-e2ff-0012 (Learnt)
    Owner ID       : 0000-5e01-1103
    Priority       : 0
    Active         : FE80::2
   Forwarder 03
    State          : Initialize
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 0
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Negative   Weight Reduced : 250
```

Display detailed information about all IPv6 VRRP groups on Device C.

```
[DeviceC] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
      Virtual IP     : FE80::10
                       1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 3 Forwarders 2 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 01
     State          : Active
     Virtual MAC    : 000f-e2ff-0011 (Take Over)
```

```
  Owner ID       : 0000-5e01-1101
  Priority       : 85
  Active         : local
  Redirect Time  : 93 secs
  Time-out Time  : 1293 secs
 Forwarder 02
  State          : Listening
  Virtual MAC    : 000f-e2ff-0012 (Learnt)
  Owner ID       : 0000-5e01-1103
  Priority       : 85
  Active         : FE80::2
 Forwarder 03
  State          : Active
  Virtual MAC    : 000f-e2ff-0013 (Owner)
  Owner ID       : 0000-5e01-1105
  Priority       : 255
  Active         : local
Forwarder Weight Track Information:
  Track Object   : 1          State : Positive   Weight Reduced : 250
```

The output shows that the weights of the VFs on Device A drop below the lower limit of failure when the uplink interface Ten-GigabitEthernet 1/0/2 of Device A fails. All VFs on Device A transit to Initialized state and cannot forward traffic. The VF for MAC address 000f-e2ff-0011 on Device C becomes the AVF to forward traffic.

4. Verify that the VF for virtual MAC address 000f-e2ff-0011 is removed from Device C when the timeout timer (about 1800 seconds) expires. The VF no longer forwards the packets destined for the MAC address.

```
[DeviceC] display vrrp ipv6 verbose
IPv6 Virtual Device Information:
 Running mode : Load balance
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 500
     Auth Type      : None
     Become Master  : 3550ms left
     Virtual IP     : FE80::10
                      1::10
     Member IP List : FE80::3 (Local, Backup)
                      FE80::1 (Master)
                      FE80::2 (Backup)
   Forwarder Information: 2 Forwarders 1 Active
     Config Weight  : 255
     Running Weight : 255
    Forwarder 02
     State          : Listening
     Virtual MAC    : 000f-e2ff-0012 (Learnt)
     Owner ID       : 0000-5e01-1103
```

```
    Priority       : 127
    Active         : FE80::2
   Forwarder 03
    State          : Active
    Virtual MAC    : 000f-e2ff-0013 (Owner)
    Owner ID       : 0000-5e01-1105
    Priority       : 255
    Active         : local
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

5. Verify that Device B has a higher priority than Device C and becomes the master when Device A fails.

```
[DeviceB] display vrrp ipv6 verbose
 IPv6 Standby Information:
    Run mode : Load balance
    Run Method     : Virtual MAC
 Total number of virtual routers : 1
  Interface Vlan-interface2
    VRID           : 1                    Adver Timer  : 1
    Admin Status   : Up                   State        : Master
    Config Pri     : 110                  Running Pri  : 110
    Preempt Mode   : Yes                  Delay Time   : 500
    Auth Type      : None
    Virtual IP     : FE80::10
                     1::10
    Member IP List : FE80::2 (Local, Master)
                     FE80::3 (Backup)
  Forwarder Information: 2 Forwarders 1 Active
    Config Weight  : 255
    Running Weight : 255
   Forwarder 02
    State          : Active
    Virtual MAC    : 000f-e2ff-0012 (Owner)
    Owner ID       : 0000-5e01-1103
    Priority       : 255
    Active         : local
   Forwarder 03
    State          : Listening
    Virtual MAC    : 000f-e2ff-0013 (Learnt)
    Owner ID       : 0000-5e01-1105
    Priority       : 127
    Active         : FE80::3
  Forwarder Weight Track Information:
    Track Object   : 1          State : Positive   Weight Reduced : 250
```

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 vrrp ipv6 mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
ipv6 address fe80::1 link-local
 ipv6 address 1::1 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 120
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface vlan-interface3
#
```

- Device B:

```
#
 vrrp ipv6 mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
ipv6 address fe80::2 link-local
 ipv6 address 1::2 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 priority 110
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface vlan-interface3
#
```

- Device C:

```
#
 vrrp ipv6 mode load-balance
#
 vlan 2 to 3
#
interface Vlan-interface2
ipv6 address fe80::3 link-local
 ipv6 address 1::3 64
undo ipv6 nd ra halt
 vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 virtual-ip 1::10
 vrrp ipv6 vrid 1 preempt-mode delay 500
 vrrp ipv6 vrid 1 weight track 1 reduced 250
#
interface Vlan-interface3
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
track 1 interface vlan-interface3
#
```

Example: Configuring VRRP with Ethernet link aggregation

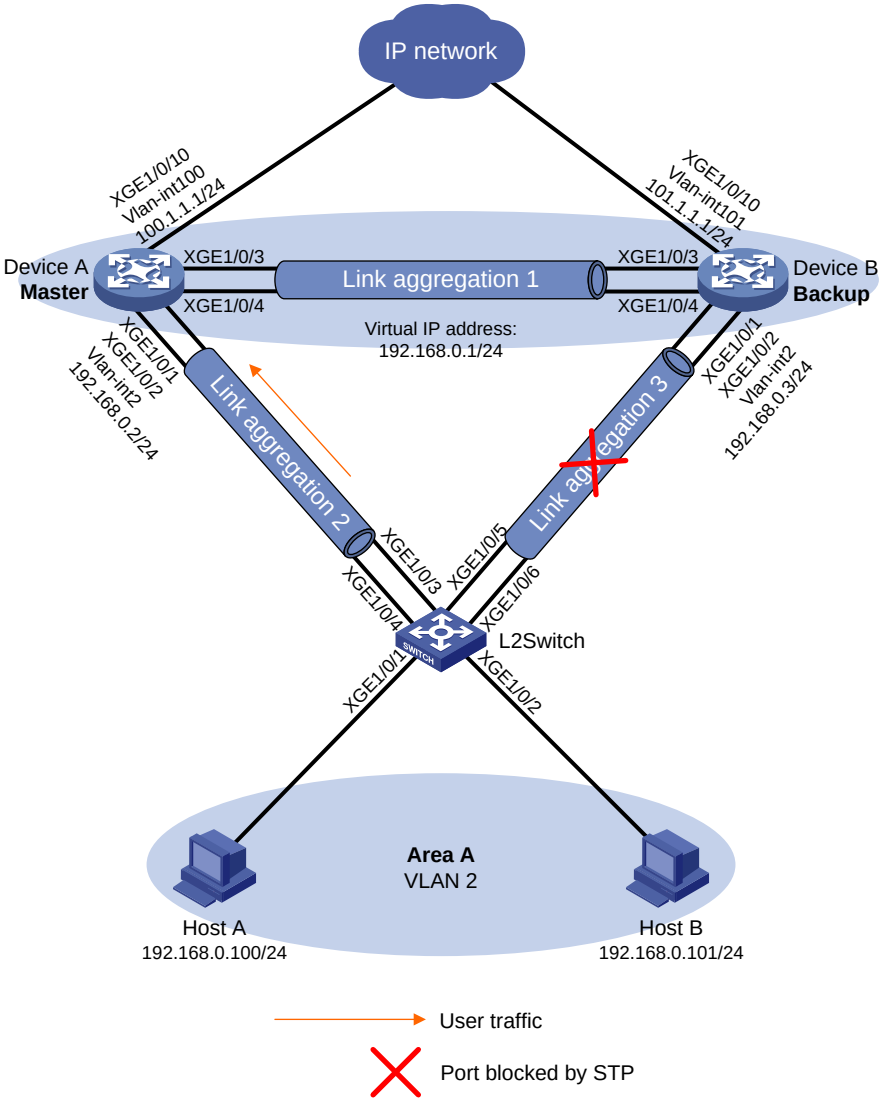
Network configuration

As shown in Figure 7, Device A, Device B, and L2switch are connected to one another through aggregate links to improve link reliability.

Configure a VRRP group on Device A and Device B as the gateway for the hosts in Area A to meet the following requirements:

- Device A operates as the master to forward packets from the hosts in Area A to the external network.
- If the uplink interface of Device A fails, the hosts in Area A can access the external network through Device B.

Figure 7 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- For Device A to become the master when it recovers from a failure, configure the preemptive mode for the VRRP group.
- For Device A to decrease its priority and become a backup when its uplink interface fails, configure VRRP tracking on Device A.
- To avoid frequent role change in the VRRP group, set a preemption delay.

- To avoid loops between Device A, Device B, and L2switch, use the spanning tree feature to block a port in the VRRP group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series	Release 63xx

Hardware	Software version
S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx

Hardware	Software version
S5135S-EI switch series	Release 6658P01 and later

Configuration restrictions and guidelines

When you configure VRRP with Ethernet link aggregation, follow these restrictions and guidelines:

- For the hosts in Area A to access the external network, make sure the following IP addresses are on the same subnet:
  - The virtual IP address of the VRRP group.
  - The downlink interface IP addresses of the VRRP group members.
- IPv4 VRRP can use VRRPv2 or VRRPv3 (default version). For a VRRP group to operate correctly, make sure the VRRP versions on all devices in the VRRP group are the same.
- Removal of the VRRP group on the IP address owner causes IP address collision. To avoid a collision, change the IP address of the interface on the IP address owner before you remove the VRRP group from the interface.
- Configure the same virtual IP addresses for each device in the VRRP group.
- Make sure the decreased priority of the master is lower than the priority of all the other devices in the VRRP group. Another device in the group can then be elected as the master.
- You must configure the same aggregation mode on both ends of an aggregate link.
- Deleting an aggregate interface also deletes the aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.
- You cannot assign a port to a Layer 2 aggregation group if any of the following features are configured on the port:
  - MAC authentication. (See *XXX Series Security Configuration Guide*.)
  - Port security. (See *XXX Series Security Configuration Guide*.)
  - 802.1X. (See *XXX Series Security Configuration Guide*.)
  - Association between AC and cross-connect. (See *XXX Series MPLS Configuration Guide*.)
  - Association between AC and VSI. (See *XXX Series VXLAN Configuration Guide*.)

Procedures

Configuring Device A

Create the Layer 2 aggregate interface Bridge-aggregation 1.

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

Assign the ports Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to Layer 2 aggregation group 1.

```
[DeviceA] interface ten-gigabitethernet 1/0/3
[DeviceA-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-Ten-GigabitEthernet1/0/3] quit
[DeviceA] interface ten-gigabitethernet 1/0/4
[DeviceA-Ten-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceA-Ten-GigabitEthernet1/0/4] quit
```

Configure Bridge-Aggregation 1 as a trunk port, and assign it to all VLANs.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan all
[DeviceA-Bridge-Aggregation1] quit
```

Create the Layer 2 aggregate interface Bridge-Aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] quit
```

Assign the ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to Layer 2 aggregation group 2.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceA-Ten-GigabitEthernet1/0/1] quit
[DeviceA] interface ten-gigabitethernet 1/0/2
[DeviceA-Ten-GigabitEthernet1/0/2] port link-aggregation group 2
[DeviceA-Ten-GigabitEthernet1/0/2] quit
```

Create VLAN 2 and VLAN-interface 2, and assign an IP address to the VLAN interface.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.2 24
[DeviceA-Vlan-interface2] quit
```

Configure Bridge-Aggregation 2 as an access port, and assign the port to VLAN 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] port link-type access
[DeviceA-Bridge-Aggregation2] port access vlan 2
[DeviceA-Bridge-Aggregation2] quit
```

Create VRRP group 1, and set its virtual IP address to 192.168.0.1.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.1
```

Set the priority of Device A to 110 in VRRP group 1. Device A has a higher priority than Device B in the VRRP group, so Device A can become the master.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure Device A to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface2] quit
```

Create track entry 1 to monitor the link status of the uplink interface Ten-GigabitEthernet 1/0/10.

```
[DeviceA] track 1 interface ten-gigabitethernet 1/0/10
```

Associate VRRP group 1 with track entry 1 and decrease the device priority by 50 when the state of track entry 1 changes to Negative.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface2] quit
```

Configure MSTP, map VLAN 2 to MSTI 1, and configure Device A as the root bridge of MSTI 1.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name vrrp
[DeviceA-mst-region] instance 1 vlan 2
```

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
[DeviceA] stp instance 1 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Configuring Device B

Create the Layer 2 aggregate interface Bridge-Aggregation 1.

```
<DeviceB> system-view
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] quit
```

Assign the ports Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to Layer 2 aggregation group 1.

```
[DeviceB] interface ten-gigabitethernet 1/0/3
[DeviceB-Ten-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceB-Ten-GigabitEthernet1/0/3] quit
[DeviceB] interface ten-gigabitethernet 1/0/4
[DeviceB-Ten-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceB-Ten-GigabitEthernet1/0/4] quit
```

Configure Bridge-Aggregation 1 as a trunk port, and assign it to all VLANs.

```
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] port link-type trunk
[DeviceB-Bridge-Aggregation1] port trunk permit vlan all
[DeviceB-Bridge-Aggregation1] quit
```

Create the Layer 2 aggregate interface Bridge-Aggregation 3.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] quit
```

Assign the ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to Layer 2 aggregation group 3.

```
[DeviceB] interface ten-gigabitethernet 1/0/1
[DeviceB-Ten-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/1] quit
[DeviceB] interface ten-gigabitethernet 1/0/2
[DeviceB-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceB-Ten-GigabitEthernet1/0/2] quit
```

Create VLAN 2 and VLAN-interface 2, and assign an IP address to the VLAN interface.

```
[DeviceB] vlan 2
[DeviceB-vlan2] quit
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 192.168.0.3 24
[DeviceB-Vlan-interface2] quit
```

Configure Bridge-Aggregation 3 as an access port, and assign the port to VLAN 2.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port link-type access
[DeviceB-Bridge-Aggregation3] port access vlan 2
[DeviceB-Bridge-Aggregation3] quit
```

Create VRRP group 1, and set its virtual IP address to 192.168.0.1.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 192.168.0.1
```

Configure Device B to operate in preemptive mode, and set the preemption delay to 5 seconds.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceB-Vlan-interface2] quit
```

Configure MSTP, map VLAN 2 to MSTI 1, and configure Device B as a secondary root bridge in MSTI 1.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name vrrp
[DeviceB-mst-region] instance 1 vlan 2
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
[DeviceB] stp instance 1 root secondary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Configuring L2switch

Create the Layer 2 aggregate interface Bridge-Aggregation 2.

```
<L2switch> system-view
[L2switch] interface bridge-aggregation 2
[L2switch-Bridge-Aggregation2] quit
```

Assign the ports Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 1/0/4 to Layer 2 aggregation group 2.

```
[L2switch] interface ten-gigabitethernet 1/0/3
[L2switch-Ten-GigabitEthernet1/0/3] port link-aggregation group 2
[L2switch-Ten-GigabitEthernet1/0/3] quit
[L2switch] interface ten-gigabitethernet 1/0/4
[L2switch-Ten-GigabitEthernet1/0/4] port link-aggregation group 2
[L2switch-Ten-GigabitEthernet1/0/4] quit
```

Create the Layer 2 aggregate interface Bridge-Aggregation 3.

```
[L2switch] interface bridge-aggregation 3
[L2switch-Bridge-Aggregation3] quit
```

Assign the ports Ten-GigabitEthernet 1/0/5 and Ten-GigabitEthernet 1/0/6 to Layer 2 aggregation group 3.

```
[L2switch] interface ten-gigabitethernet 1/0/5
[L2switch-Ten-GigabitEthernet1/0/5] port link-aggregation group 3
[L2switch-Ten-GigabitEthernet1/0/5] quit
[L2switch] interface ten-gigabitethernet 1/0/6
[L2switch-Ten-GigabitEthernet1/0/6] port link-aggregation group 3
[L2switch-Ten-GigabitEthernet1/0/6] quit
```

Create VLAN 2, configure Bridge-Aggregation 2 and Bridge-Aggregation 3 as access ports, and assign the aggregate interfaces to VLAN 2.

```
[L2switch] vlan 2
[L2switch-vlan2] quit
[L2switch] interface bridge-aggregation 2
```

```
[L2switch-Bridge-Aggregation2] port access vlan 2
[L2switch-Bridge-Aggregation2] quit
[L2switch] interface bridge-aggregation 3
[L2switch-Bridge-Aggregation3] port access vlan 2
[L2switch-Bridge-Aggregation3] quit
```

Set the MST region name of the device to **vrrp**.

```
[L2switch] stp region-configuration
[L2switch-mst-region] region-name vrrp
```

Map VLAN 2 to MSTI 1, and activate the MST region configuration.

```
[L2switch-mst-region] instance 1 vlan 2
[L2switch-mst-region] active region-configuration
[L2switch-mst-region] quit
```

Enable the spanning tree feature globally.

```
[L2switch] stp global enable
```

Verifying the configuration

1. Verify that the hosts with routes configured can ping the external network.

   # Verify that Host A can ping the IP address 20.1.1.1 in the external network.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 20.1.1.1

Pinging 20.1.1.1 with 32 bytes of data:
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 20.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Verify that Device A is operating as the master and Device B as the backup in VRRP group 1. Device A forwards packets from the hosts in Area A to the external network.

   # Display detailed information about all VRRP groups on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : Not supported
```

```
      Version       : 3
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
   VRRP Track Information:
     Track Object   : 1                   State : Positive   Pri Reduced : 50
```

Display detailed information about all VRRP groups on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                   Adver Timer  : 100
     Admin Status   : Up                  State        : Backup
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 500
     Become Master  : 2950ms left
     Auth Type      : Not supported
      Version       : 3
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
```

3. Verify that link aggregation groups are successfully configured on Device A, Device B, and L2switch.

Display brief information about all Layer 2 aggregate interfaces on Device A.

```
[DeviceA] display interface Bridge-Aggregation brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                UP   20G(a)   F(a)   T    1
BAGG2                UP   20G(a)   F(a)   A    2
```

Display brief information about all Layer 2 aggregate interfaces on Device B.

```
[DeviceB] display interface Bridge-Aggregation brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                UP   20G(a)   F(a)   T    1
BAGG3                UP   20G(a)   F(a)   A    2
```

Display brief information about all Layer 2 aggregate interfaces on L2switch.

```
[L2switch] display interface Bridge-Aggregation brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
```

```
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG2                UP   20G(a)   F(a)   A    2
BAGG3                UP   20G(a)   F(a)   A    2
```

The output shows that the speed of each aggregate link is 20 Gbps, and the bandwidth is twice the bandwidth of each physical link.

4. Verify that Host A can still ping the IP address 20.1.1.1 after the uplink interface Ten-GigabitEthernet 1/0/10 of Device A fails.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hostA>ping 20.1.1.1

Pinging 20.1.1.1 with 32 bytes of data:
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128
Reply from 20.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 20.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5. Verify that Device B takes over to forward packets from the hosts in Area A to the external network after Ten-GigabitEthernet 1/0/10 of Device A fails.

Display detailed information about all VRRP groups on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 110               Running Pri  : 60
     Preempt Mode   : Yes               Delay Time   : 500
     Become Master  : 3350ms left
     Auth Type      : Not supported
      Version       : 3
     Virtual IP     : 192.168.0.1
     Master IP      : 192.168.0.3
   VRRP Track Information:
     Track Object   : 1                 State : Negative   Pri Reduced : 50
```

Display detailed information about all VRRP groups on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
```

```
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : Not supported
      Version       : 3
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.3
```

6. Verify that Device A becomes the master to forward packets from the hosts in Area A to the external network when Ten-GigabitEthernet 1/0/10 recovers.

Display detailed information about all VRRP groups on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 110               Running Pri  : 110
     Preempt Mode   : Yes               Delay Time   : 500
     Auth Type      : Not supported
      Version       : 3
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 50
```

Display detailed information about all VRRP groups on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 500
     Become Master  : 2950ms left
     Auth Type      : Not supported
      Version       : 3
     Virtual IP     : 192.168.0.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 192.168.0.2
```

Configuration files

- Device A:

```
#
 sysname DeviceA
#
vlan 2
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp instance 1 root primary
stp global enable
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface Bridge-Aggregation2
 port access vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 50
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/4
  port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
track 1 interface Ten-GigabitEthernet1/0/10
#
```

- Device B:

```
#
 sysname DeviceB
#
vlan 2
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp instance 1 root secondary
stp global enable
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface Bridge-Aggregation2
 port access vlan 2
#
interface Vlan-interface2
 ip address 192.168.0.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
vrrp vrid 1 preempt-mode delay 500
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
```

```
interface Ten-GigabitEthernet1/0/4
  port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
```

- L2switch:

```
#
 sysname L2switch
#
vlan 2
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp global enable
#
interface Bridge-Aggregation2
 port access vlan 2
#
interface Bridge-Aggregation3
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 2
#
interface Ten-GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 2
 port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 2
```

```
 port link-aggregation group 3
#
```

Contents

Introduction

This document provides BFD configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of BFD, VRRP, Track, OSPF, and IS-IS.

Example: Configuring VRRP-BFD-Track collaboration

Network configuration

As shown in Figure 1:

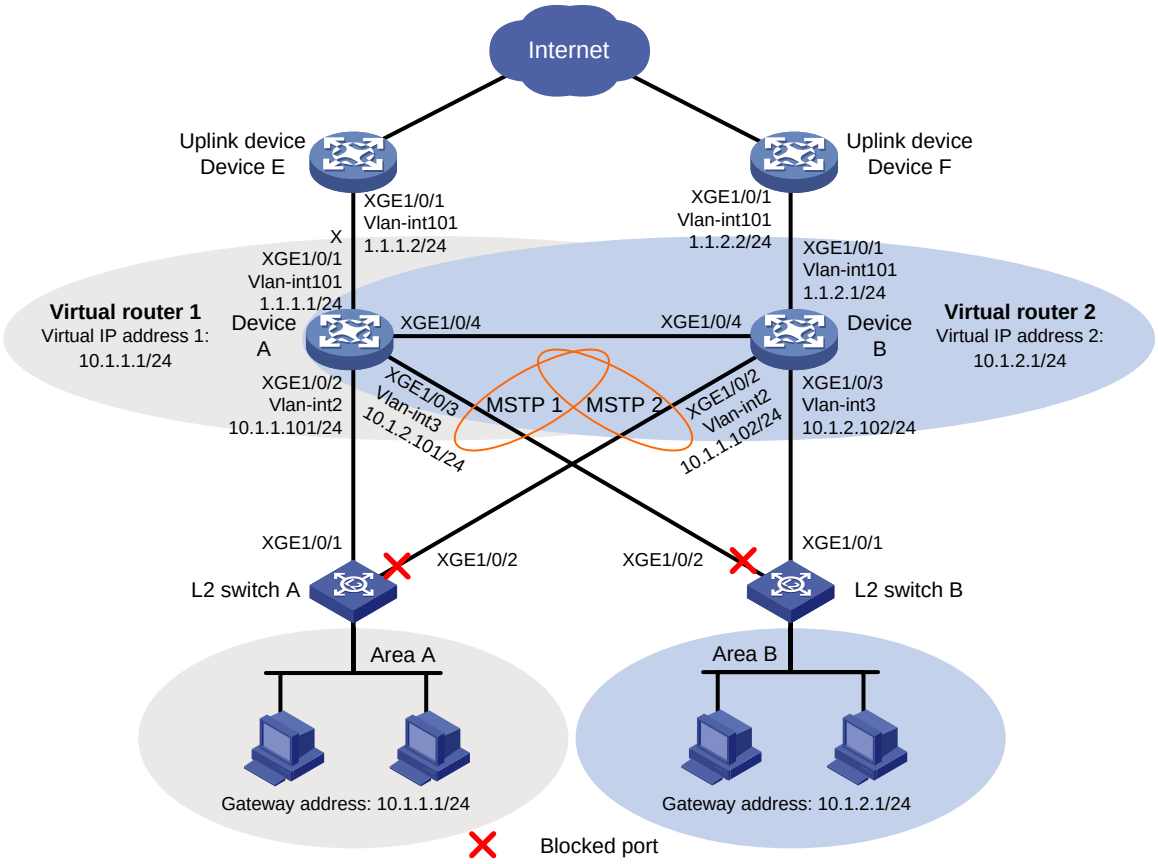
- Two distribution layer devices, Device A and Device B, are deployed at the egress of area A and area B.
- Device A and Device B belong to VRRP group 1 and VRRP group 2.
- Device A is the master in VRRP group 1. Device B is the master in VRRP group 2.
- The default gateway is VRRP group 1 for users in area A and VRRP group 2 for users in area B.

Configure VRRP-Track-BFD collaboration to meet the following requirements:

When Device A and Device B are operating correctly, they forward traffic for users in area A and area B, respectively.

- When one gateway device or the uplink of the device fails, BFD can detect the failure and the other device takes over to implement link switchover.
- When the downlink of a gateway device fails, L2 Switch A or L2 Switch B forwards user traffic to the gateway through interface GigabitEthernet 1/0/2. When the fault is cleared, L2 Switch A or L2 Switch B forwards user traffic to the gateway through interface GigabitEthernet 1/0/1.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- For Device A to become the master in VRRP group 1, configure a higher priority (110) for Device A in VRRP group 1 (Device B uses the default priority 100). For Device B to become the master in VRRP group 2, configure a higher priority (110) for Device B in VRRP group 2 (Device A uses the default priority 100).
- To enable the failed master to forward traffic when it recovers, configure both VRRP groups to operate in preemptive mode.
- To enable Device A to communicate with Device B by using VRRP advertisement packets and BFD packets of different VLANs, configure the ports connecting Device A and Device B to allow packets from VLAN 2 and VLAN 3 to pass through.
- To eliminate Layer 2 loops, configure MSTP. Map VLAN 2 to MSTI 1 and map VLAN 3 to MSTI 2. The configuration traffic in MSTI 1 and MSTI 2 is forwarded through GigabitEthernet 1/0/1 of L2 Switch A and GigabitEthernet 1/0/1 of L2 Switch B, respectively.
- To prevent MSTP from blocking uplink interface GigabitEthernet 1/0/1 of Device A and Device B, disable the spanning tree feature on the interfaces.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V3-EI switch series	Release 63xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI	Not supported

S5120V3-54P-PWR-SI	
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 63xx
S3600V3-SI switch series	Release 11xx
S5120V2-SI switch series S5120V2-LI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx
WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure VRRP-BFD-Track collaboration, follow these restrictions and guidelines:

- Make sure the VRRP versions on all devices of the VRRP group are the same.

- The source IP address for BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.
- The virtual IP address of an IPv4 VRRP group and the downlink interface IP address of the VRRP group must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 101
[DeviceA-vlan101] port gigabitethernet 1/0/1
[DeviceA-vlan101] quit
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ip address 1.1.1.1 24
[DeviceA-Vlan-interface101] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring the interfaces that connect the gateways

1. Configure Device A:

   # Configure GigabitEthernet 1/0/4 as a trunk port, remove the interface from VLAN 1, and assign it to VLAN 2 and VLAN 3.

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-type trunk
[DeviceA-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/4] port trunk permit vlan 2 to 3
[DeviceA-GigabitEthernet1/0/4] port trunk pvid vlan 2
[DeviceA-GigabitEthernet1/0/4] quit
```

2. Configure Device B:

   # Configure GigabitEthernet 1/0/4 as a trunk port, remove the interface from VLAN 1, and assign it to VLAN 2 and VLAN 3.

```
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-type trunk
[DeviceB-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/4] port trunk permit vlan 2 to 3
[DeviceB-GigabitEthernet1/0/4] port trunk pvid vlan 2
[DeviceB-GigabitEthernet1/0/4] quit
```

Disabling the spanning tree feature on uplink interfaces

1. Disable the spanning tree feature on GigabitEthernet 1/0/1 of Device A:

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

2. Disable the spanning tree feature on GigabitEthernet 1/0/1 of Device B:

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configuring static routes from Device E and Device F to the virtual IP addresses of the VRRP groups

1. Configure Device E:

   Configure static routes to the virtual IP addresses of VRRP group 1 and VRRP group 2.

```
<DeviceE> system-view
[DeviceE] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
[DeviceE] ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
```

2. Configure Device F:

   Configure static routes to the virtual IP addresses of VRRP group 1 and VRRP group 2.

```
<DeviceE> system-view
[DeviceF] ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
[DeviceF] ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
```

Configuring VRRP groups

1. Configure Device A:

   # Configure the virtual IP address for VRRP group 1, set the preemption delay, and configure the priority of Device A in VRRP group 1.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceA-Vlan-interface2] vrrp vrid 1 priority 110
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface2] quit
```

   # Configure the virtual IP address for VRRP group 2, and set the preemption delay.

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceA-Vlan-interface3] vrrp vrid 2 preempt-mode delay 500
[DeviceA–Vlan-interface3] quit
```

2. Configure Device B:

   # Configure the virtual IP address for VRRP group 1, and set the preemption delay.

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[DeviceB-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
[DeviceB-Vlan-interface2] quit
```

   # Configure the virtual IP address for VRRP group 2, set the preemption delay, and configure the priority of Device B in VRRP group 2.

```
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] vrrp vrid 2 virtual-ip 10.1.2.1
[DeviceB-Vlan-interface3] vrrp vrid 2 priority 110
[DeviceB-Vlan-interface3] vrrp vrid 2 preempt-mode delay 500
[DeviceB–Vlan-interface3] quit
```

Configuring BFD

1. Configure Device A:

   # Configure the source IP address for BFD echo packets.

   ```
   [DeviceA] bfd echo-source-ip 10.10.10.10
   ```

2. Configure Device B:

   # Configure the source IP address for BFD echo packets.

   ```
   [DeviceB] bfd echo-source-ip 11.11.11.11
   ```

Configuring Track

1. Configure Device A:

   # Create track entry 1, and associate it with the BFD session to verify the reachability of Device E.

   ```
   [DeviceA] track 1 bfd echo interface vlan-interface 101 remote ip 1.1.1.2 local ip 1.1.1.1
   [DeviceA-track-1] quit
   ```

   # Associate VRRP group 1 with track entry 1 and decrease the router priority by 20 when the state of track entry 1 changes to negative.

   ```
   [DeviceA] interface vlan-interface 2
   [DeviceA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 20
   [DeviceA-Vlan-interface2] quit
   ```

2. Configure Device B:

   # Create track entry 1, and associate it with the BFD session to verify the reachability of Device F.

   ```
   [DeviceB] track 1 bfd echo interface vlan-interface 101 remote ip 1.1.2.2 local ip 1.1.2.1
   [DeviceB-track-1] quit
   ```

   # Associate VRRP group 2 with track entry 1 and decrease the router priority by 20 when the state of track entry 1 changes to negative.

   ```
   [DeviceB] interface vlan-interface 3
   [DeviceB-Vlan-interface3] vrrp vrid 2 track 1 priority reduced 20
   [DeviceB-Vlan-interface3] quit
   ```

Configuring MSTP

1. Configure Device A:

   ```
   [DeviceA] stp region-configuration
   [DeviceA-mst-region] region-name vrrp
   [DeviceA-mst-region] instance 1 vlan 2
   [DeviceA-mst-region] instance 2 vlan 3
   [DeviceA-mst-region] active region-configuration
   [DeviceA-mst-region] quit
   [DeviceA] stp instance 1 root primary
   [DeviceA] stp instance 2 root secondary
   [DeviceA] stp global enable
   ```

2. Configure Device B:

   ```
   [DeviceB] stp region-configuration
   ```

```
[DeviceB-mst-region] region-name vrrp
[DeviceB-mst-region] instance 1 vlan 2
[DeviceB-mst-region] instance 2 vlan 3
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
[DeviceB] stp instance 2 root primary
[DeviceB] stp instance 1 root secondary
[DeviceB] stp global enable
```

3. Configure L2 Switch A:

```
<SwitchA> system-view
[SwitchA] stp region-configuration
[SwitchA-mst-region] region-name vrrp
[SwitchA-mst-region] instance 1 vlan 2
[SwitchA-mst-region] active region-configuration
[SwitchA-mst-region] quit
[SwitchA] stp global enable
```

4. Configure L2 Switch B:

```
<SwitchB> system-view
[SwitchB] stp region-configuration
[SwitchB-mst-region] region-name vrrp
[SwitchB-mst-region] instance 2 vlan 3
[SwitchB-mst-region] active region-configuration
[SwitchB-mst-region] quit
[SwitchB] stp global enable
```

Verifying the configuration

1. Verify that the hosts in the LAN can access the external network when Device A and Device B are operating correctly:

   # Ping 1.1.1.2 from host A in area A.

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

   # Ping 1.1.2.2 from host C in area B.

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
```

```
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

The output shows that the hosts in area A and area B can access the external network.

Display BFD session information on Device A.

```
[DeviceA] display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:

 LD             SourceAddr      DestAddr        State    Holdtime    Interface
 129            1.1.1.1         1.1.1.2         Up       500ms       Vlan101
```

The output shows that a BFD session has been established.

Display detailed VRRP group information on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID            : 1                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 110               Running Pri  : 110
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.1.1
     Virtual MAC     : 0000-5e00-0101
     Master IP       : 10.1.1.101
   VRRP Track Information:
     Track Object    : 1                 State : Positive   Pri Reduced : 20

   Interface Vlan-interface3
     VRID            : 2                 Adver Timer  : 100
     Admin Status    : Up                State        : Backup
     Config Pri      : 100               Running Pri  : 100
     Preempt Mode    : Yes               Delay Time   : 500
     Become Master   : 3600ms left
     Auth Type       : None
     Virtual IP      : 10.1.2.1
     Virtual MAC     : 0000-5e00-0102
     Master IP       : 10.1.2.102
```

Display detailed VRRP group information on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
```

```
Interface Vlan-interface2
  VRID            : 1                   Adver Timer  : 100
  Admin Status    : Up                  State        : Backup
  Config Pri      : 100                 Running Pri  : 100
  Preempt Mode    : Yes                 Delay Time   : 500
  Become Master   : 3100ms left
  Auth Type       : None
  Virtual IP      : 10.1.1.1
  Virtual MAC     : 0000-5e00-0101
  Master IP       : 10.1.1.101

Interface Vlan-interface3
  VRID            : 2                   Adver Timer  : 100
  Admin Status    : Up                  State        : Master
  Config Pri      : 110                 Running Pri  : 110
  Preempt Mode    : Yes                 Delay Time   : 500
  Auth Type       : None
  Virtual IP      : 10.1.2.1
  Virtual MAC     : 0000-5e00-0102
  Master IP       : 10.1.2.102
VRRP Track Information:
  Track Object    : 1                   State : Positive   Pri Reduced : 20
```

The output shows the following information:

- In VRRP group 1, Device A is the master, and Device B is the backup. Hosts that use default gateway 10.1.1.1/24 access the Internet through Device A.
- In VRRP group 2, Device B is the master, and Device A is the backup. Hosts that use default gateway 10.1.2.1/24 access the Internet through Device B.

2. Verify that the hosts in the LAN can access the external network when the uplink monitored by Device A fails:

Ping 1.1.1.2 from host A in area A.

```
<host A> ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
56 bytes from 1.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 1.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

Ping 1.1.2.2 from host C in area B.

```
<host C> ping 1.1.2.2
PING 1.1.2.2 (1.1.2.2): 56 data bytes
56 bytes from 1.1.2.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 1.1.2.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 1.1.2.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 1.1.2.2: seq=3 ttl=128 time=7.45 ms
```

```
56 bytes from 1.1.2.2: seq=4 ttl=128 time=9.11 ms

--- 1.1.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.17/11.01/22.43 ms
```

The output shows that the hosts in area A and area B can access the external network.

Display BFD session information on Device A.

```
[DeviceA] display bfd session

 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 session working in echo mode:

 LD             SourceAddr      DestAddr        State    Holdtime    Interface
 129            1.1.1.1         1.1.1.2         Down        /        Vlan101
```

The output shows that the BFD session has been terminated.

Display detailed VRRP group information on Device B.

```
[DeviceB] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID            : 1                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 100               Running Pri  : 100
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.1.1
     Virtual MAC     : 0000-5e00-0101
     Master IP       : 10.1.1.102

   Interface Vlan-interface3
     VRID            : 2                 Adver Timer  : 100
     Admin Status    : Up                State        : Master
     Config Pri      : 110               Running Pri  : 110
     Preempt Mode    : Yes               Delay Time   : 500
     Auth Type       : None
     Virtual IP      : 10.1.2.1
     Virtual MAC     : 0000-5e00-0102
     Master IP       : 10.1.2.102
   VRRP Track Information:
     Track Object    : 1                 State : Positive   Pri Reduced : 20
```

The output shows that Device B becomes the master in VRRP group 1. Hosts in area A access the external network through Device B.

When the fault is cleared, display BFD session information on Device A.

```
[DeviceA] display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active
```

```
 IPv4 session working in echo mode:

 LD              SourceAddr      DestAddr        State    Holdtime    Interface
 129             1.1.1.1         1.1.1.2         Up       1000ms      Vlan101
```

The output shows that the BFD session is resumed.

Display detailed VRRP group information on Device A.

```
[DeviceA] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode      : Standard
 Total number of virtual routers : 2
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer  : 100
     Admin Status   : Up                 State        : Master
     Config Pri     : 110                Running Pri  : 110
     Preempt Mode   : Yes                Delay Time   : 500
     Auth Type      : None
     Virtual IP     : 10.1.1.1
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.101
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 20

   Interface Vlan-interface3
     VRID           : 2                  Adver Timer  : 100
     Admin Status   : Up                 State        : Backup
     Config Pri     : 100                Running Pri  : 100
     Preempt Mode   : Yes                Delay Time   : 500
     Become Master  : 3550ms left
     Auth Type      : None
     Virtual IP     : 10.1.2.1
     Virtual MAC    : 0000-5e00-0102
     Master IP      : 10.1.2.102
```

The output shows that Device A resumes its priority and becomes the master in VRRP group 1 again. Hosts in area B access the external network through Device A.

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 bfd echo-source-ip 10.10.10.10
#
vlan 2 to 3
#
vlan 101
```

```
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 instance 2 vlan 3
 active region-configuration
#
 stp instance 1 root primary
 stp instance 2 root secondary
 stp global enable
#
interface Vlan-interface2
 ip address 10.1.1.101 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 20
#
interface Vlan-interface3
 ip address 10.1.2.101 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.2.1
 vrrp vrid 2 preempt-mode delay 500
#
interface Vlan-interface101
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 3
 port trunk pvid vlan 2
#
 track 1 bfd echo interface Vlan-interface101 remote ip 1.1.1.2 local ip 1.1.1.1
```

- Device B:

```
#
 bfd echo-source-ip 11.11.11.11
#
vlan 2 to 3
#
vlan 101
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 instance 2 vlan 3
 active region-configuration
#
 stp instance 1 root secondary
 stp instance 2 root primary
 stp global enable
#
interface Vlan-interface2
 ip address 10.1.1.102 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.1
 vrrp vrid 1 preempt-mode delay 500
#
interface Vlan-interface3
 ip address 10.1.2.102 255.255.255.0
 vrrp vrid 2 virtual-ip 10.1.2.1
 vrrp vrid 2 priority 110
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 1 priority reduced 20
#
interface Vlan-interface101
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 3
 port trunk pvid vlan 2
#
 track 1 bfd echo interface Vlan-interface101 remote ip 1.1.2.2 local ip 1.1.2.1
```

- L2 Switch A:

```
#
vlan 2
#
stp region-configuration
 region-name vrrp
 instance 1 vlan 2
 active region-configuration
#
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
```

- L2 Switch B:

```
#
vlan 3
#
stp region-configuration
 region-name vrrp
 instance 2 vlan 3
 active region-configuration
#
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
```

- Device E:

```
#
vlan 101
#
interface Vlan-interface101
 ip address 1.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
 ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
 ip route-static 10.1.2.0 255.255.255.0 1.1.1.1
```

- Device F:

```
#
vlan 101
#
interface Vlan-interface101
 ip address 1.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
 ip route-static 10.1.1.0 255.255.255.0 1.1.2.1
 ip route-static 10.1.2.0 255.255.255.0 1.1.2.1
```

Example: Configuring BFD for static routing

Network configuration

As shown in Figure 2:

- Device A has two paths to reach Device B: one over a Layer 2 switch, and the other over Device C.
- A Layer 2 switch connects Device A and Device B.

Because Device B does not support BFD, enable BFD echo packet mode on Device A. When the link between Device B and the Layer 2 switch fails, Device A switches the path over Device C to reach Device B.

Figure 2 Network diagram

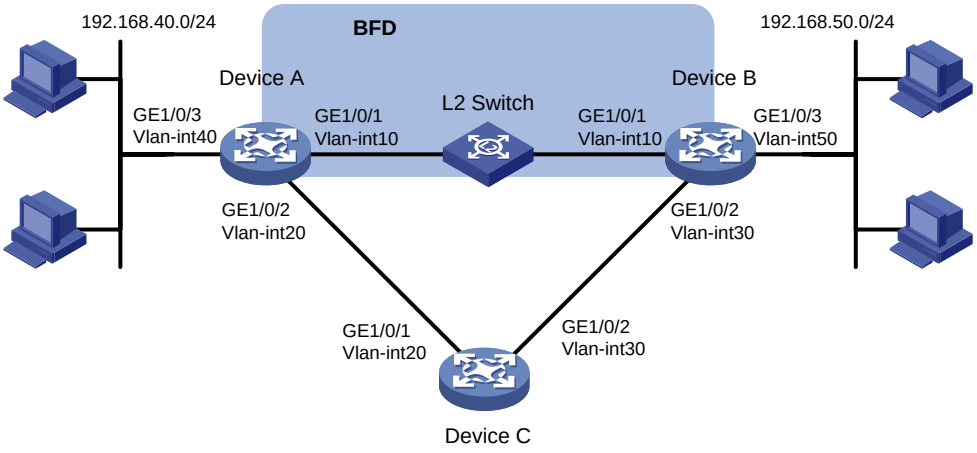


Table 1 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int10	192.168.10.101/24
Device A	Vlan-int20	192.168.20.101/24
Device A	Vlan-int40	192.168.40.101/24
Device B	Vlan-int10	192.168.10.102/24
Device B	Vlan-int30	192.168.30.101/24
Device B	Vlan-int50	192.168.50.101/24
Device C	Vlan-int20	192.168.20.102/24
Device C	Vlan-int30	192.168.30.102/24

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx,

	Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch	Release 63xx
E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported

WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

The source IP address for BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 192.168.10.101 24
[DeviceA-Vlan-interface10] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring static routes

1. Configure Device A:

   # Configure two static routes with the same destination network 192.168.50.0/24 and different preferences. Configure the BFD echo packet mode for the preferred static route (Device A –> L2 Switch–> Device B).

```
[DeviceA] ip route-static 192.168.50.0 24 vlan-interface 10 192.168.10.102 bfd
echo-packet
[DeviceA] ip route-static 192.168.50.0 24 vlan-interface 20 192.168.20.102
preference 65
```

2. Configure Device B:

   # Configure two static routes with the same destination network 192.168.40.0/24 and different preferences. Configure the BFD echo packet mode for the preferred static route (Device B –> L2 Switch–> Device A).

```
[DeviceB] ip route-static 192.168.40.0 24 vlan-interface 10 192.168.10.101
```

```
[DeviceB] ip route-static 192.168.40.0 24 vlan-interface 30 192.168.30.102
preference 65
```

3. Configure Device C:

Configure static routes with destination networks 192.168.40.0/24 and 192.168.50.0/24.

```
[DeviceC] ip route-static 192.168.40.0 24 vlan-interface 20 192.168.20.101
[DeviceC] ip route-static 192.168.50.0 24 vlan-interface 30 192.168.30.101
```

Configuring BFD parameters on Device A

Configure the source IP address for BFD echo packets.

```
[DeviceA] bfd echo-source-ip 10.10.10.10
```

Configure the minimum interval for receiving BFD echo packets and the single-hop detection time multiplier.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] bfd min-echo-receive-interval 100
[DeviceA-Vlan-interface10] bfd detect-multiplier 3
[DeviceA-Vlan-interface10] quit
```

Verifying the configuration

1. Verify the configuration when Device A and Device B and the link between them are operating correctly:

Display static route information on Device A.

```
[DeviceA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.50.0/24     Static 60   0            192.168.10.102  Vlan10

Static Routing table Status : <Inactive>
Summary Count : 0
```

The output shows that Device A communicates with Device B through the Layer 2 switch.

Display BFD session information on Device A.

```
[DeviceA] display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:

 LD          SourceAddr      DestAddr        State    Holdtime    Interface
 67          192.168.10.101  192.168.10.102  Up       300ms       Vlan10
```

The output shows that a BFD session has been established.

2. Verify the configuration when the link between Device B and the Layer 2 switch is faulty:

Display static route information on Device A.

```
[DeviceA] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
192.168.50.0/24     Static 65   0            192.168.20.102  Vlan20

Static Routing table Status : <Inactive>
Summary Count : 0
```

The output shows that Device A communicates with Device B through Device C.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 bfd echo-source-ip 10.10.10.10
#
vlan 10
#
vlan 20
#
vlan 40
#
interface Vlan-interface10
 ip address 192.168.10.101 255.255.255.0
 bfd min-echo-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface20
 ip address 192.168.20.101 255.255.255.0
#
interface Vlan-interface40
 ip address 192.168.40.101 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

```
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 40
#
 ip route-static 192.168.50.0 24 Vlan-interface10 192.168.10.102 bfd echo-packet
 ip route-static 192.168.50.0 24 Vlan-interface20 192.168.20.102 preference 65
#
```

- Device B:

```
#
vlan 10
#
vlan 30
#
vlan 50
#
interface Vlan-interface10
 ip address 192.168.10.102 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.30.101 255.255.255.0
#
interface Vlan-interface50
 ip address 192.168.50.101 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 50
#
 ip route-static 192.168.40.0 24 Vlan-interface10 192.168.10.101
 ip route-static 192.168.40.0 24 Vlan-interface30 192.168.30.102 preference 65
#
```

- Device C:

```
#
vlan 20
#
vlan 30
#
interface Vlan-interface20
 ip address 192.168.20.102 255.255.255.0
#
```

```
interface Vlan-interface30
 ip address 192.168.30.102 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
 ip route-static 192.168.40.0 24 Vlan-interface20 192.168.20.101
 ip route-static 192.168.50.0 24 Vlan-interface30 192.168.30.101
#
```

Example: Configuring BFD for RIP

Network configuration

As shown in Figure 3, Device A, Device B, and Device C run RIP. Device A and Device C are connected through a Layer 2 switch.

Enable BFD echo packet mode on Device A (Device C does not support BFD) to monitor the path over the Layer 2 switch. When BFD detects a link failure, it notifies RIP to switch to the path over Device B.

Figure 3 Network diagram

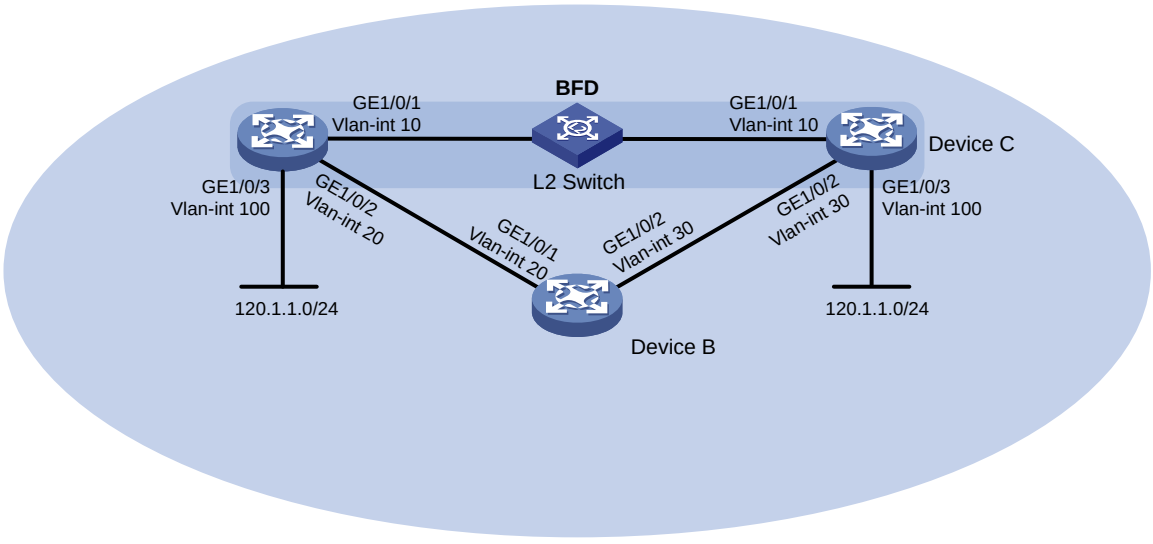


Table 2 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int10	10.1.0.101/24
Device A	Vlan-int20	192.168.0.101/24
Device A	Vlan-int100	120.1.1.1/24

Device	Interface	IP address
Device B	Vlan-int20	192.168.0.102/24
Device B	Vlan-int30	13.1.1.101/24
Device C	Vlan-int10	10.1.0.102/24
Device C	Vlan-int30	13.1.1.102/24
Device C	Vlan-int100	121.1.1.1/24

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch	Release 63xx
E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Release 63xx

IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

The source IP address for BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface10
[DeviceA-Vlan-interface10] ip address 10.1.0.101 24
[DeviceA-Vlan-interface10] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring RIP

1. Configure Device A:

   # Configure basic RIP functions, import direct routes, and enable BFD for RIP.

```
<DeviceA> system-view
[DeviceA] rip 1
[DeviceA-rip-1] version 2
[DeviceA-rip-1] undo summary
[DeviceA-rip-1] network 10.1.0.0
[DeviceA-rip-1] network 192.168.0.0
[DeviceA-rip-1] import-route direct
[DeviceA-rip-1] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] rip bfd enable
[DeviceA-Vlan-interface10] quit
```

2. Configure Device B:

   # Configure basic RIP functions, and import direct routes.

```
<DeviceB> system-view
[DeviceB] rip 1
```

```
[DeviceB-rip-1] version 2
[DeviceB-rip-1] undo summary
[DeviceB-rip-1] network 192.168.0.0
[DeviceB-rip-1] network 13.1.1.0
[DeviceB-rip-1] import-route direct
[DeviceB-rip-1] quit
```

3. Configure Device C:

Configure basic RIP functions, and import direct routes.

```
<DeviceC> system-view
[DeviceC] rip 1
[DeviceC-rip-1] version 2
[DeviceC-rip-1] undo summary
[DeviceC-rip-1] network 10.1.0.0
[DeviceC-rip-1] network 13.1.1.0
[DeviceC-rip-1] import-route direct
[DeviceC-rip-1] quit
```

Configuring BFD parameters on Device A

Configure the source IP address for BFD echo packets.

```
[DeviceA] bfd echo-source-ip 11.11.11.11
```

Configure the minimum interval for receiving BFD echo packets and the single-hop detection time multiplier.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] bfd min-echo-receive-interval 100
[DeviceA-Vlan-interface10] bfd detect-multiplier 3
[DeviceA-Vlan-interface10] quit
```

Verifying the configuration

Display BFD session information on Device A.

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:
       Local Discr: 2049
         Source IP: 10.1.0.101          Destination IP: 10.1.0.102
     Session State: Up                       Interface: Vlan-interface10
         Hold Time: 300ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 0                        Tx Count: 910
      Connect Type: Direct             Running Up for: 00:00:46
       Detect Mode: Async                       Slot: 1
          Protocol: RIP
           Version: 1
         Diag Info: No Diagnostic
```

The output shows that a BFD session has been established and is up.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 10.1.0.102
      Flags: 0x1008c       OrigNextHop: 10.1.0.102
      Label: NULL          RealNextHop: 10.1.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface10
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 1              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 10.1.0.102
      Flags: 0x1008c       OrigNextHop: 10.1.0.102
      Label: NULL          RealNextHop: 10.1.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface10
BkTunnel ID: Invalid       BkInterface: N/A
```

```
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0               MicroSegID: 0
```

The output shows that Device A communicates with Device C through the Layer 2 switch.

When the link between Device C and the Layer 2 switch fails, view BFD log information.

```
%Oct  9 18:42:17:650 2013 Device A BFD/5/BFD_CHANGE_FSM: Sess[10.1.0.101/10.1.0.102,
LD/RD:2049/2049, Interface:Vlan10, SessType:Echo, LinkType:INET], Ver:1, Sta: UP->
DOWN, Diag:1 (Control Detection Time Expired)
```

The output shows that BFD can quickly detect the failure and notify RIP.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP
 Process ID: 2
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x26000002         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 192.168.0.102
      Flags: 0x1008c        OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface20
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

(Release 63xx, 6008 and later, and 8005 and later) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 24 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: RIP
 Process ID: 2
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
```

```
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 192.168.0.102
      Flags: 0x1008c        OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface20
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0               MicroSegID: 0
```

The output shows that Device A communicates with Device C through Device B.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 bfd echo-source-ip 11.11.11.11
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
 network 192.168.0.0
 import-route direct
#
vlan 10
#
vlan 20
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.101 255.255.255.0
 rip bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface20
 ip address 192.168.0.101 255.255.255.0
#
interface Vlan-interface100
 ip address 120.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

- Device B:

```
#
rip 1
 undo summary
 version 2
 network 192.168.0.0
network 13.1.1.0
 import-route direct
#
vlan 20
#
vlan 30
#
interface Vlan-interface20
 ip address 192.168.0.102 255.255.255.0
#
interface Vlan-interface30
 ip address 13.1.1.101 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
```

- Device C:

```
#
rip 1
 undo summary
 version 2
 network 10.1.0.0
network 13.1.1.0
 import-route direct
```

```
#
vlan 10
#
vlan 30
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
#
interface Vlan-interface30
 ip address 13.1.1.102 255.255.255.0
#
interface Vlan-interface100
 ip address 121.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

Example: Configuring BFD for OSPF

Network configuration

As shown in Figure 4, Device A, Device B, and Device C run OSPF. Device A and Device C are connected through a Layer 2 switch.

Enable BFD control packet mode on Device A and Device C to monitor the path over the Layer 2 switch. When BFD detects a link failure, it notifies OSPF to switch to the path over Device B.

Figure 4 Network diagram

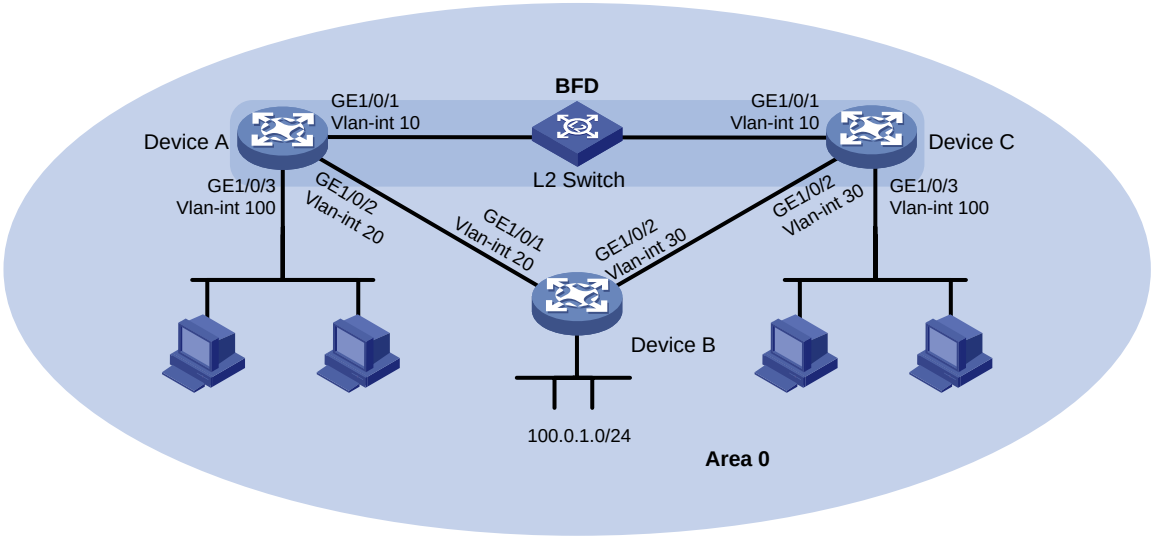


Table 3 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int10	10.1.0.101/24
Device A	Vlan-int20	192.168.0.101/24
Device A	Vlan-int100	120.1.1.1/24
Device B	Vlan-int20	192.168.0.102/24
Device B	Vlan-int30	13.1.1.101/24
Device C	Vlan-int10	10.1.0.102/24
Device C	Vlan-int30	13.1.1.102/24
Device C	Vlan-int100	121.1.1.1/24

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx,

	Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx

S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

In BFD control packet mode, a minimum of one end must operate in active mode for a BFD session to be established.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.0.101 24
[DeviceA-Vlan-interface10] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring OSPF

1. Configure Device A:

   # Configure basic OSPF functions, and enable BFD for OSPF.

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 120.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ospf bfd enable
[DeviceA-Vlan-interface10] quit
```

2. Configure Device B:

   # Configure basic OSPF functions.

```
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

3. Configure Device C:

   # Configure basic OSPF functions, and enable BFD for OSPF.

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 121.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] ospf bfd enable
[DeviceC-Vlan-interface10] quit
```

Configuring BFD parameters

1. Configure Device A:

   # Configure the session establishment mode as active (this is the default mode).

```
[DeviceA] bfd session init-mode active
```

   # Configure the minimum interval for sending and receiving single-hop BFD control packets and the single-hop detection time multiplier.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] bfd min-transmit-interval 100
[DeviceA-Vlan-interface10] bfd min-receive-interval 100
[DeviceA-Vlan-interface10] bfd detect-multiplier 3
```

```
[DeviceA-Vlan-interface10] quit
```

2. Configure Device C:

Configure the session establishment mode as active (this is the default mode).

```
[DeviceC] bfd session init-mode active
```

Configure the minimum interval for sending and receiving single-hop BFD control packets and the single-hop detection time multiplier.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] bfd min-transmit-interval 100
[DeviceC-Vlan-interface10] bfd min-receive-interval 100
[DeviceC-Vlan-interface10] bfd detect-multiplier 3
[DeviceC-Vlan-interface10] quit
```

Verifying the configuration

Ping host C (connected to Device C) from host A (connected to Device A) to verify the connectivity.

```
<host A> ping 121.1.1.2
PING 121.1.1.2 (121.1.1.2): 56 data bytes
56 bytes from 121.1.1.2: seq=0 ttl=128 time=22.43 ms
56 bytes from 121.1.1.2: seq=1 ttl=128 time=7.17 ms
56 bytes from 121.1.1.2: seq=2 ttl=128 time=8.91 ms
56 bytes from 121.1.1.2: seq=3 ttl=128 time=7.45 ms
56 bytes from 121.1.1.2: seq=4 ttl=128 time=9.11 ms

--- 121.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/std-dev = 7.17/11.01/22.43 ms
```

The output shows that host C can be pinged successfully.

Display detailed OSPF neighbor information on Device A.

```
[DeviceA] display ospf peer verbose

          OSPF Process 1 with Router ID 2.2.2.2
                  Neighbors

 Area 0.0.0.0 interface 10.1.0.101(Vlan-interface10)'s neighbors
 Router ID: 1.1.1.1          Address: 10.1.0.102       GR State: Normal
   State: Full  Mode: Nbr is Slave  Priority: 1
   DR: 10.1.0.101  BDR: 10.1.0.102  MTU: 0
   Options is 0x42 (-|O|-|-|-|E|-)
   Dead timer due in 39  sec
   Neighbor is up for 00:09:01
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
   BFD status: Enabled(Control mode)
```

The output shows that Device A has established OSPF neighbor relationship with Device C.

Display BFD session information on Device A and Device C.

```
[DeviceA] display bfd session verbose
```

```
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:
       Local Discr: 2049                 Remote Discr: 2049
         Source IP: 10.1.0.101         Destination IP: 10.1.0.102
     Session State: Up                      Interface: Vlan-interface10
      Min Tx Inter: 100ms                 Act Tx Inter: 100ms
      Min Rx Inter: 100ms                 Detect Inter: 300ms
      Rx Count: 536                       Tx Count: 536
      Connect Type: Direct              Running Up for: 00:04:48
         Hold Time: 300ms                     Auth mode: None
        Detect Mode: Async                         Slot: 1
           Protocol: OSPF
            Version: 1
         Diag Info: No Diagnostic
[DeviceC] display bfd session verbose
 Total Session Num: 1    Up Session Num: 1    Init Mode: Active

 IPv4 session working in control packet mode:
       Local Discr: 2049                 Remote Discr: 2049
         Source IP: 10.1.0.102         Destination IP: 10.1.0.101
     Session State: Up                      Interface: Vlan-interface10
      Min Tx Inter: 100ms                 Act Tx Inter: 100ms
      Min Rx Inter: 100ms                 Detect Inter: 300ms
          Rx Count: 3971                      Tx Count: 3776
      Connect Type: Direct              Running Up for: 00:06:52
         Hold Time: 300ms                     Auth mode: None
        Detect Mode: Async                         Slot: 1
           Protocol: OSPF
            Version: 1
         Diag Info: No Diagnostic
```

The output shows that BFD sessions have been established and are up.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: OSPF
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1               Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
```

```
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

(Release 65xx, 6008 and later, 8005 and later, 11xx, and 6615Pxx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: OSPF
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 1               Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0               MicroSegID: 0
```

The output shows that Device A communicates with Device C through the Layer 2 switch.

When the link between Device C and the Layer 2 switch fails, view BFD log information.

```
%Oct  9 15:22:23:154 2013 DeviceC BFD/5/BFD_CHANGE_FSM: Sess[10.1.0.102/10.1.0.101,
LD/RD:2049/2049, Interface:Vlan10, SessType:Ctrl, LinkType:INET], Ver:1, Sta: UP->
DOWN, Diag: 1 (Control Detection Time Expired)
%Oct  9 15:22:23:155 2013 DeviceC OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor
10.1.0.101(Vlan-interface10) from FULL to DOWN.
```

The output shows that BFD can quickly detect the failure and notify OSPF.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1
```

```
Destination: 121.1.1.0/24
   Protocol: OSPF
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x26000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.0.102
      Label: NULL          RealNextHop: 192.168.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface20
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: OSPF
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x26000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.0.102
      Label: NULL          RealNextHop: 192.168.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface20
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
   LinkCost: 0               MicroSegID: 0
```

The output shows that Device A communicates with Device C through Device B.

Configuration files

NOTE:
Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 120.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.101 255.255.255.0
 ospf bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface20
 ip address 192.168.0.101 255.255.255.0
#
interface Vlan-interface100
 ip address 120.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

- Device B:

```
#
ospf 1
```

```
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
vlan 20
#
vlan 30
#
interface Vlan-interface20
 ip address 192.168.0.102 255.255.255.0
#
interface Vlan-interface30
 ip address 13.1.1.101 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
  network 121.1.1.0 0.0.0.255
#
vlan 10
#
vlan 30
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
 ospf bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface30
 ip address 13.1.1.102 255.255.255.0
#
interface Vlan-interface100
 ip address 121.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

Example: Configuring BFD for IS-IS

Network configuration

As shown in Figure 5, Device A, Device B, and Device C run IS-IS. Device A and Device C are connected through a Layer 2 switch.

Enable BFD control packet mode on Device A and Device C to monitor the path over the Layer 2 switch. When BFD detects a link failure, it notifies IS-IS to switch to the path over Device B.

Figure 5 Network diagram

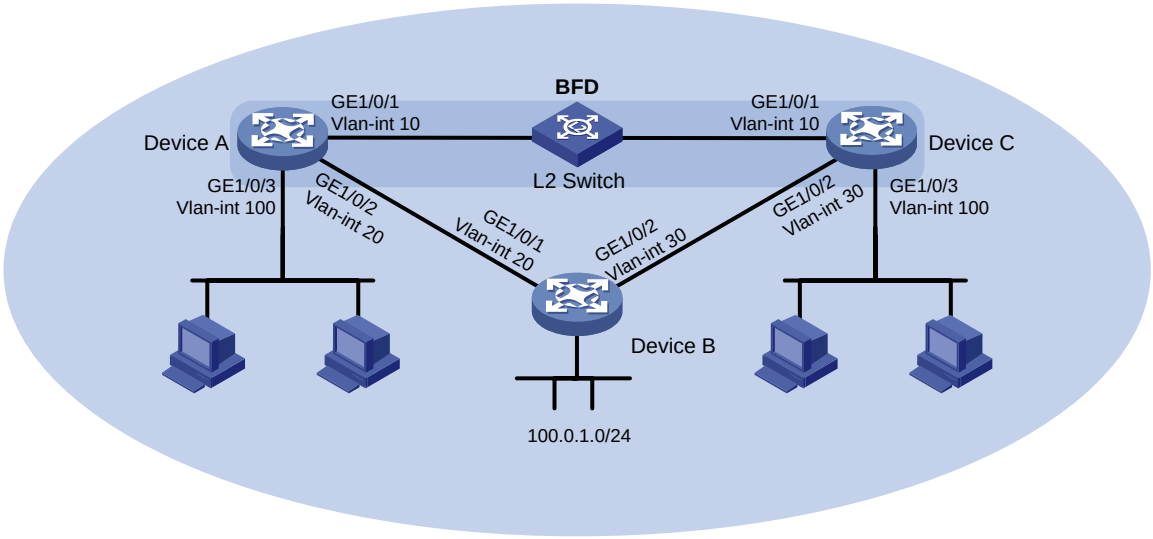


Table 4 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int10	10.1.0.101/24
Device A	Vlan-int20	192.168.0.101/24
Device A	Vlan-int100	120.1.1.1/24
Device B	Vlan-int20	192.168.0.102/24

Device	Interface	IP address
Device B	Vlan-int30	13.1.1.101/24
Device C	Vlan-int10	10.1.0.102/24
Device C	Vlan-int30	13.1.1.102/24
Device C	Vlan-int100	121.1.1.1/24

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

S5500V3-48P-SI	
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch	Not supported

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

In BFD control packet mode, a minimum of one end must operate in active mode for a BFD session to be established.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.0.101 24
[DeviceA-Vlan-interface10] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring IS-IS

1. Configure Device A:

   # Configure basic IS-IS functions, and enable BFD for IS-IS.

```
[DeviceA] isis
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] isis enable
[DeviceA-Vlan-interface20] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] isis enable
[DeviceA-Vlan-interface10] isis bfd enable
[DeviceA-Vlan-interface10] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] isis enable
[DeviceA-Vlan-interface100] isis bfd enable
[DeviceA-Vlan-interface100] quit
```

2. Configure Device B:

   # Configure basic IS-IS functions.

```
[DeviceB] isis
[DeviceB-isis-1] network-entity 10.0000.0000.0003.00
```

```
[DeviceB-isis-1] quit
[DeviceB] interface vlan-interface 20
[DeviceB-Vlan-interface20] isis enable
[DeviceB-Vlan-interface20] quit
[DeviceB] interface vlan-interface 30
[DeviceB-Vlan-interface30] isis enable
[DeviceB-Vlan-interface30] quit
```

3. Configure Device C:

Configure basic IS-IS functions, and enable BFD for IS-IS.

```
[DeviceC] isis
[DeviceC-isis-1] network-entity 10.0000.0000.0002.00
[DeviceC-isis-1] quit
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] isis enable
[DeviceC-Vlan-interface10] isis bfd enable
[DeviceC-Vlan-interface10] quit
[DeviceC] interface vlan 30
[DeviceC-Vlan-interface30] isis enable
[DeviceC-Vlan-interface30] quit
[DeviceC] interface vlan-interface 100
[DeviceC-Vlan-interface100] isis enable
[DeviceC-Vlan-interface100] isis bfd enable
[DeviceC-Vlan-interface100] quit
```

Configuring BFD parameters

1. Configure Device A:

Configure the session establishment mode as active (this is the default mode).

```
[DeviceA] bfd session init-mode active
```

Configure the minimum interval for sending and receiving single-hop BFD control packets and the single-hop detection time multiplier.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] bfd min-transmit-interval 100
[DeviceA-Vlan-interface10] bfd min-receive-interval 100
[DeviceA-Vlan-interface10] bfd detect-multiplier 3
[DeviceA-Vlan-interface10] quit
```

2. Configure Device C:

Configure the session establishment mode as active (this is the default mode).

```
[DeviceC] bfd session init-mode active
```

Configure the minimum interval for sending and receiving single-hop BFD control packets and the single-hop detection time multiplier.

```
[DeviceC] interface vlan 10
[DeviceC-Vlan-interface10] bfd min-transmit-interval 100
[DeviceC-Vlan-interface10] bfd min-receive-interval 100
[DeviceC-Vlan-interface10] bfd detect-multiplier 3
[DeviceC-Vlan-interface10] quit
```

Verifying the configuration

Display detailed IS-IS neighbor information on Device A.

```
[DeviceA] display isis peer verbose

                        Peer information for IS-IS(1)
                        ------------------------------


 System ID: 0000.0000.0002
 Interface: Vlan10                 Circuit Id:  0000.0000.0002.01
 State: Up    HoldTime: 6s         Type: L1(L1L2)     PRI: 64
 Area address(es): 00
 Peer IP address(es): 10.1.0.102
 Peer local circuit ID: 1
 Peer circuit SNPA address: ce9d-d91d-d100
 Uptime: 00:01:19
 Adj protocol:  IPv4
 Graceful Restart capable
   Restarting signal: No
   Suppress adjacency advertisement: No
 Local topology:
   0
 Remote topology:
   0
```

The output shows that Device A has established IS-IS neighbor relationship with Device C.

Display BFD session information on Device A and Device C.

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:
       Local Discr: 2049                Remote Discr: 2049
         Source IP: 10.1.0.101         Destination IP: 10.1.0.102
     Session State: Up                      Interface: Vlan-interface10
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 3                        Tx Count: 3
      Connect Type: Direct             Running Up for: 00:06:09
         Hold Time: 300ms                   Auth mode: None
       Detect Mode: Async                        Slot: 1
          Protocol: ISIS_BR_L1/ISIS_BR_L2
           Version: 1
         Diag Info: No Diagnostic
[DeviceC] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:
       Local Discr: 2049                Remote Discr: 2049
```

```
        Source IP: 10.1.0.102         Destination IP: 10.1.0.101
     Session State: Up                     Interface: Vlan-interface10
      Min Tx Inter: 100ms                Act Tx Inter: 100ms
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 3                        Tx Count: 3
      Connect Type: Direct             Running Up for: 00:07:10
         Hold Time: 300ms                   Auth mode: None
       Detect Mode: Async                       Slot: 1
          Protocol: ISIS_BR_L1/ISIS_BR_L2
           Version: 1
         Diag Info: No Diagnostic
```

The output shows that BFD sessions have been established and are up.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: IS_L1
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 20               Preference: 15
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                     State: Active Adv
  OrigTblID: 0x2                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c         OrigNextHop: 10.1.0.102
      Label: NULL            RealNextHop: 10.1.0.102
    BkLabel: NULL              BkNextHop: N/A
    SRLabel: NULL              BkSRLabel: NULL
  Tunnel ID: Invalid           Interface: Vlan-interface10
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                  PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: IS_L1
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 20               Preference: 15
      IpPre: N/A              QosLocalID: N/A
```

```
        Tag: 0                   State: Active Adv
  OrigTblID: 0x2                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0                MicroSegID: 0
```

The output shows that Device A communicates with Device C through the Layer 2 switch.

When the link between Device C and the Layer 2 switch fails, view BFD log information.

```
%Oct  9 16:11:24:163 2013 DeviceC BFD/5/BFD_CHANGE_FSM: Sess[10.1.0.102/10.1.0.101,
LD/RD:2049/2049, Interface:Vlan10, SessType:Ctrl, LinkType:INET], Ver:1, Sta: UP->
DOWN, Diag: 1 (Control Detection Time Expired)
%Oct  9 16:11:24:164 2013 DeviceC ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency
0000.0000.0001 (Vlan-interface10), state changed to DOWN, Reason: BFD session down.
%Oct  9 16:11:24:164 2013 DeviceC ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-2 adjacency
0000.0000.0001 (Vlan-interface10), state changed to DOWN, Reason: BFD session down.
```

The output shows that BFD can quickly detect the failure and notify IS-IS.

(Release 63xx) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: IS_L1
 Process ID: 1
  SubProtID: 0x1                    Age: 04h20m37s
       Cost: 2               Preference: 10
      IpPre: N/A             QosLocalID: N/A
        Tag: 0                   State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x26000002          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x1008c        OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface20
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
```

```
  Connector: N/A                PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 121.1.1.0/24 on Device A.

```
<DeviceA> display ip routing-table 121.1.1.0 verbose

Summary Count : 1

Destination: 121.1.1.0/24
   Protocol: IS_L1
 Process ID: 1
  SubProtID: 0x1                  Age: 04h20m37s
       Cost: 2              Preference: 10
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0              OrigVrf: default-vrf
    TableID: 0x2               OrigAs: 0
      NibID: 0x26000002        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.0.102
      Label: NULL          RealNextHop: 192.168.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
   SIDIndex: NULL              InLabel: NULL
  Tunnel ID: Invalid           Interface: Vlan-interface20
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0          TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
   LinkCost: 0               MicroSegID: 0
```

The output shows that Device A communicates with Device C through Device B.

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
isis 1
 network-entity 10.0000.0000.0001.00
#
vlan 10
#
vlan 20
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.101 255.255.255.0
```

```
isis enable 1
 isis bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface20
 ip address 192.168.0.101 255.255.255.0
isis enable 1
#
interface Vlan-interface100
 ip address 120.1.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

- Device B:

```
#
isis 1
 network-entity 10.0000.0000.0003.00
#
vlan 20
#
vlan 30
#
interface Vlan-interface20
 ip address 192.168.0.102 255.255.255.0
isis enable 1
#
interface Vlan-interface30
 ip address 13.1.1.101 255.255.255.0
isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 30
#
```

- Device C:

```
#
isis 1
 network-entity 10.0000.0000.0002.00
#
vlan 10
#
vlan 30
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
isis enable 1
 isis bfd enable
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface30
 ip address 13.1.1.102 255.255.255.0
isis enable 1
#
interface Vlan-interface100
 ip address 121.1.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

Example: Configuring BFD for BGP

Network configuration

As shown in Figure 6, the devices in AS 100 run OSPF to reach each other. There are two paths between Device B and Device D:

- **Path A**—Path over Device C.
- **Path B**—Path over Device E.

When both paths are available, BGP uses the path over Device C to forward traffic between Device A and Device F.

Enable BFD control packet mode on Device B and Device D to monitor the path over Device C. When BFD detects a link failure, it notifies BGP to switch to the path over Device E.

Figure 6 Network diagram

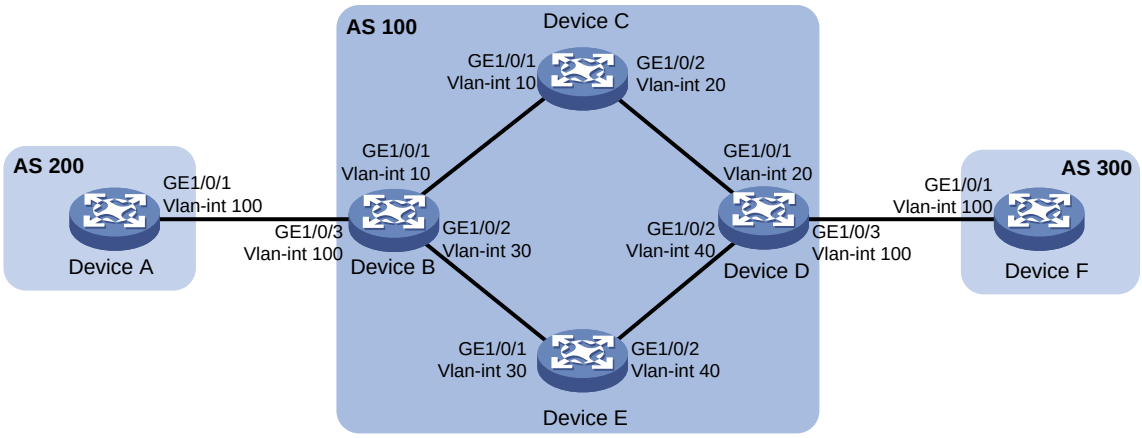


Table 5 Interface and IP address assignment

Device	Interface	IP address
Device A	Vlan-int100	120.1.0.1/24
Device B	Vlan-int10	10.1.0.101/24
Device B	Vlan-int30	192.168.0.101/24
Device B	Vlan-int100	120.1.0.2/24
Device C	Vlan-int10	10.1.0.102/24
Device C	Vlan-int20	10.2.0.102/24
Device D	Vlan-int20	10.2.0.101/24
Device D	Vlan-int40	13.1.1.101/24
Device D	Vlan-int100	120.2.0.2/24
Device E	Vlan-int30	192.168.0.102/24
Device E	Vlan-int40	13.1.1.102/24
Device F	Vlan-int100	120.2.0.1/24

Analysis

For Path A to become the primary path, use a routing policy to set a lower cost for Path A than Path B.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported

S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series	Not supported
E128C switch E152C switch	Release 63xx
E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

In BFD control packet mode, a minimum of one end must operate in active mode for a BFD session to be established.

Procedures

Configuring interface IP addresses

Configure IP addresses for the interfaces on the devices. (Details not shown.)

Configuring OSPF in AS 100

1. Configure Device B:

```
[DeviceB] ospf
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
```

```
[DeviceB-ospf-1] quit
```

2. Configure Device C:

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

3. Configure Device D:

```
[DeviceD] ospf
[DeviceD-ospf-1] import-route direct
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.2.0.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

4. Configure Device E:

```
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

Configuring BGP

1. Configure Device A:

   # Enable BGP and set the local AS number to 200.

```
[DeviceA] bgp 200
[DeviceA-bgp-default] router-id 1.1.1.1
```

   # Establish an EBGP connection with Device B.

```
[DeviceA-bgp-default] peer 120.1.0.2 as-number 100
```

   # Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceA-bgp-default] address-family ipv4 unicast
```

   # In BGP IPv4 unicast address family view, inject local network 120.1.0.0/24 to the BGP routing table.

```
[DeviceA-bgp-default-ipv4] network 120.1.0.0 255.255.255.0
```

   # Enable BGP to exchange IPv4 unicast routing information with peer 120.1.0.2.

```
[DeviceA-bgp-default-ipv4] peer 120.1.0.2 enable
[DeviceA-bgp-default-ipv4] quit
```

2. Configure Device B:

   # Enable BGP and set the local AS number to 100.

```
[DeviceB] bgp 100
[DeviceB-bgp-default] router-id 2.2.2.2
```

   # Establish an EBGP connection with Device A.

```
[DeviceB-bgp-default] peer 120.1.0.1 as-number 200
```

   # Establish IBGP connections with Device D.

```
[DeviceB-bgp-default] peer 10.2.0.101 as-number 100
[DeviceB-bgp-default] peer 13.1.1.101 as-number 100
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceB-bgp-default] address-family ipv4 unicast
```

Enable BGP to exchange IPv4 unicast routing information with peer 10.2.0.101.

```
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 enable
```

In BGP IPv4 unicast address family view, specify the device as the next hop for routes sent to peer 10.2.0.101.

```
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 next-hop-local
```

Enable BGP to exchange IPv4 unicast routing information with peer 13.1.1.101.

```
[DeviceB-bgp-default-ipv4] peer 13.1.1.101 enable
```

In BGP IPv4 unicast address family view, specify the device as the next hop for routes sent to peer 13.1.1.101.

```
[DeviceB-bgp-default-ipv4] peer 13.1.1.101 next-hop-local
```

Enable BGP to exchange IPv4 unicast routing information with peer 120.1.0.1.

```
[DeviceB-bgp-default-ipv4] peer 120.1.0.1 enable
[DeviceB-bgp-default-ipv4] quit
```

3. Configure Device D:

Enable BGP and set the local AS number to 100.

```
[DeviceD] bgp 100
[DeviceD-bgp-default] router-id 4.4.4.4
```

Establish IBGP connections with Device B.

```
[DeviceD-bgp-default] peer 10.1.0.101 as-number 100
[DeviceD-bgp-default] peer 192.168.0.101 as-number 100
```

Establish an EBGP connection with Device F.

```
[DeviceD-bgp-default] peer 120.2.0.1 as-number 300
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceD-bgp-default] address-family ipv4 unicast
```

Enable BGP to exchange IPv4 unicast routing information with peer 10.1.0.101.

```
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 enable
```

In BGP IPv4 unicast address family view, specify the device as the next hop for routes sent to peer 10.1.0.101.

```
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 next-hop-local
```

Enable BGP to exchange IPv4 unicast routing information with peer 192.168.0.101.

```
[DeviceD-bgp-default-ipv4] peer 192.168.0.101 enable
```

In BGP IPv4 unicast address family view, specify the device as the next hop for routes sent to peer 192.168.0.101.

```
[DeviceD-bgp-default-ipv4] peer 192.168.0.101 next-hop-local
```

Enable BGP to exchange IPv4 unicast routing information with peer 120.2.0.1.

```
[DeviceD-bgp-default-ipv4] peer 120.2.0.1 enable
[DeviceD-bgp-default-ipv4] quit
```

4. Configure Device F:

Enable BGP and set the local AS number to 300.

```
[DeviceF] bgp 300
[DeviceF-bgp-default] router-id 6.6.6.6
```

Establish an EBGP connection with Device D.

```
[DeviceF-bgp-default] peer 120.2.0.2 as-number 100
```

Create the BGP IPv4 unicast address family and enter its view.

```
[DeviceF-bgp-default] address-family ipv4 unicast
```

In BGP IPv4 unicast address family view, inject local network 120.2.0.0/24 to the BGP routing table.

```
[DeviceF-bgp-default-ipv4] network 120.2.0.0 255.255.255.0
```

Enable BGP to exchange IPv4 unicast routing information with peer 120.2.0.2.

```
[DeviceF-bgp-default-ipv4] peer 120.2.0.2 enable
[DeviceF-bgp-default-ipv4] quit
```

Configuring routing policies

1. Configure Device B:

Create ACL 2000 to permit packets sourced from 120.1.0.0/24.

```
[DeviceB] acl basic 2000
[DeviceB-acl-ipv4-basic-2000] rule permit source 120.1.0.0 0.0.0.255
[DeviceB-acl-ipv4-basic-2000] quit
```

Set a local preference of 200 for routes advertised to peer 10.2.0.101, and set the preference for IBGP routes to 100.

```
[DeviceB] route-policy local-pre permit node 10
[DeviceB-route-policy-local-pre] if-match ip address acl 2000
[DeviceB-route-policy-local-pre] apply local-preference 200
[DeviceB-route-policy-local-pre] quit
[DeviceB] bgp 100
[DeviceB-bgp-default] address-family ipv4 unicast
[DeviceB-bgp-default-ipv4] peer 10.2.0.101 route-policy local-pre export
[DeviceB-bgp-default-ipv4] preference 255 100 130
[DeviceB-bgp-default-ipv4] quit
```

2. Configure Device D:

Create ACL 2000 to permit packets sourced from 120.2.0.0/24.

```
[DeviceD] acl basic 2000
[DeviceD-acl-ipv4-basic-2000] rule permit source 120.2.0.0 0.0.0.255
[DeviceD-acl-ipv4-basic-2000] quit
```

Set a local preference of 200 for routes learned from peer 10.1.0.101, and configure the preference for IBGP routes as 100.

```
[DeviceD] route-policy local-pre permit node 10
[DeviceD-route-policy-local-pre] if-match ip address acl 2000
[DeviceD-route-policy-local-pre] apply local-preference 200
[DeviceD-route-policy-local-pre] quit
[DeviceD] bgp 100
[DeviceD-bgp-default] address-family ipv4 unicast
[DeviceD-bgp-default-ipv4] peer 10.1.0.101 route-policy local-pre export
[DeviceD-bgp-default-ipv4] preference 255 100 130
[DeviceD-bgp-default-ipv4] quit
```

Configuring BFD

1. Configure Device B:

Enable BFD for the link to BGP peer 10.2.0.101.

```
[DeviceB] bgp 100
[DeviceB-bgp-default] peer 10.2.0.101 bfd
[DeviceB-bgp-default] quit
```

2. Configure Device D:

Enable BFD for the link to BGP peer 10.1.0.101.

```
[DeviceD] bgp 100
[DeviceD-bgp-default] peer 10.1.0.101 bfd
[DeviceD-bgp-default] quit
```

Verifying the configuration

Ping Device F from Device A to verify the connectivity.

```
[DeviceA] ping 120.2.0.1
Ping 120.2.0.1 (120.2.0.1): 56 data bytes, press CTRL+C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=1.189 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=1.095 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=1.086 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=1.097 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=1.089 ms

--- Ping statistics for 120.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.086/1.111/1.189/0.039 ms
```

The output shows that Device F can be pinged successfully.

Display BGP peer information on Device B.

```
[DeviceB] display bgp peer ipv4

 BGP local router ID: 2.2.2.2
 Local AS number: 100
 Total number of peers: 3                 Peers in established state: 3

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.0.101              100        6        4    0       1 00:00:56 Established
  13.1.1.101              100        6        5    0       1 00:00:56 Established
  120.1.0.1               200        6        5    0       1 00:00:56 Established
```

The output shows the following information:

- Two IBGP connections have been established between Device B and Device D.
- An EBGP connection has been established between Device B and Device A.

Display detailed BFD session information on Device B.

```
[DeviceB] display bfd session verbose
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 session working in control packet mode:
       Local Discr: 2049                Remote Discr: 0
```

```
         Source IP: 10.1.0.101         Destination IP: 10.2.0.101
     Session State: UP                      Interface: N/A
         Hold Time: 0ms                 Act Tx Inter: 400ms
      Min Rx Inter: 400ms               Detect Inter: 2000ms
          Rx Count: 0                       Tx Count: 910
      Connect Type: Indirect           Running Up for: 00:00:00
       Detect Mode: Async                       Slot: 1
          Protocol: BGP
           Version: 1
         Diag Info: No Diagnostic
```

The output shows that a BFD session has been established and is up.

(Release 63xx) Display information about the routes to network 120.2.0.0/24 on Device B.

```
[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 3

Destination: 120.2.0.0/24
   Protocol: BGP instance default
 Process ID: 0
  SubProtID: 0x1                    Age: 00h24m48s
       Cost: 0                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 300
      NibID: 0x15000001          LastAs: 300
     AttrID: 0x1               Neighbor: 10.2.0.101
      Flags: 0x10060        OrigNextHop: 10.2.0.101
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                    Age: 00h26m19s
       Cost: 1                Preference: 150
      IpPre: N/A              QosLocalID: N/A
        Tag: 1                    State: Inactive Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x13000005          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 10.1.0.102
```

```
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                  Age: 00h26m19s
       Cost: 1              Preference: 150
      IpPre: N/A            QosLocalID: N/A
        Tag: 1                  State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x13000003         LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface30
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 120.2.0.0/24 on Device B.

```
[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 3

Destination: 120.2.0.0/24
   Protocol: BGP instance default
 Process ID: 0
  SubProtID: 0x1                  Age: 00h24m48s
       Cost: 0              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                  State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 300
      NibID: 0x15000001         LastAs: 300
     AttrID: 0x1              Neighbor: 10.2.0.101
      Flags: 0x10060        OrigNextHop: 10.2.0.101
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
```

```
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
   LinkCost: 0               MicroSegID: 0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                   Age: 00h26m19s
       Cost: 1               Preference: 150
      IpPre: N/A             QosLocalID: N/A
        Tag: 1                   State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x13000005          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 10.1.0.102
      Label: NULL           RealNextHop: 10.1.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface10
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0
   LinkCost: 0               MicroSegID: 0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                   Age: 00h26m19s
       Cost: 1               Preference: 150
      IpPre: N/A             QosLocalID: N/A
        Tag: 1                   State: Inactive Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 0
      NibID: 0x13000003          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface30
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
```

```
  Connector: N/A                PathID: 0x0
   LinkCost: 0              MicroSegID: 0
```

The output shows that Device B communicates with Device D through path over Device C.

When the path over Device C fails, ping Device F from Device A.

```
[DeviceA] ping 120.2.0.1
Ping 120.1.0.1 (120.2.0.1): 56 data bytes, press CTRL+C to break
56 bytes from 120.2.0.1: icmp_seq=0 ttl=252 time=0.680 ms
56 bytes from 120.2.0.1: icmp_seq=1 ttl=252 time=0.295 ms
56 bytes from 120.2.0.1: icmp_seq=2 ttl=252 time=0.423 ms
56 bytes from 120.2.0.1: icmp_seq=3 ttl=252 time=0.464 ms
56 bytes from 120.2.0.1: icmp_seq=4 ttl=252 time=0.445 ms

--- Ping statistics for 120.2.0.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.295/0.461/0.680/0.124 ms
```

The output shows that Device F can be pinged successfully.

(Release 63xx) Display information about the routes to network 120.2.0.0/24 on Device B.

```
[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 2

Destination: 120.2.0.0/24
   Protocol: BGP instance default
 Process ID: 0
  SubProtID: 0x1                  Age: 00h00m18s
       Cost: 0              Preference: 100
      IpPre: N/A            QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0               OrigVrf: default-vrf
    TableID: 0x2                OrigAs: 300
      NibID: 0x15000001         LastAs: 300
     AttrID: 0x1              Neighbor: 13.1.1.101
      Flags: 0x10060       OrigNextHop: 13.1.1.101
      Label: NULL          RealNextHop: 192.168.0.102
    BkLabel: NULL            BkNextHop: N/A
    SRLabel: NULL            BkSRLabel: NULL
  Tunnel ID: Invalid         Interface: Vlan-interface30
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                PathID: 0x0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                  Age: 00h00m18s
       Cost: 1              Preference: 150
      IpPre: N/A            QosLocalID: N/A
```

```
        Tag: 1                    State: Inactive Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x13000001          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface30
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
```

(Release 65xx, 6008 and later, and 8005 and later) Display information about the routes to network 120.2.0.0/24 on Device B.

```
[DeviceB] display ip routing-table 120.2.0.0 24 verbose

Summary Count : 2

Destination: 120.2.0.0/24
   Protocol: BGP instance default
 Process ID: 0
  SubProtID: 0x1                    Age: 00h00m18s
       Cost: 0                Preference: 100
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active Adv
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 300
      NibID: 0x15000001          LastAs: 300
     AttrID: 0x1                Neighbor: 13.1.1.101
      Flags: 0x10060         OrigNextHop: 13.1.1.101
      Label: NULL            RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid          Interface: Vlan-interface30
BkTunnel ID: Invalid        BkInterface: N/A
   FtnIndex: 0x0           TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0               MicroSegID: 0

Destination: 120.2.0.0/24
   Protocol: O_ASE2
 Process ID: 1
  SubProtID: 0x8                    Age: 00h00m18s
       Cost: 1                Preference: 150
      IpPre: N/A              QosLocalID: N/A
        Tag: 1                    State: Inactive Adv
```

```
  OrigTblID: 0x0                OrigVrf: default-vrf
    TableID: 0x2                 OrigAs: 0
      NibID: 0x13000001          LastAs: 0
     AttrID: 0xffffffff        Neighbor: 0.0.0.0
      Flags: 0x41           OrigNextHop: 192.168.0.102
      Label: NULL           RealNextHop: 192.168.0.102
    BkLabel: NULL             BkNextHop: N/A
    SRLabel: NULL             BkSRLabel: NULL
   SIDIndex: NULL               InLabel: NULL
  Tunnel ID: Invalid           Interface: Vlan-interface30
BkTunnel ID: Invalid         BkInterface: N/A
   FtnIndex: 0x0            TrafficIndex: N/A
  Connector: N/A                 PathID: 0x0
   LinkCost: 0                MicroSegID: 0
```

The output shows that Device B communicates with Device D through path over Device E.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 120.1.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
bgp 200
 router-id 1.1.1.1
 peer 120.1.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.1.0.0 255.255.255.0
  peer 120.1.0.2 enable
#
```

- Device B:

```
#
ospf 1
import-route direct
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
```

```
#
vlan 10
#
vlan 30
#
vlan 100
#
interface Vlan-interface10
 ip address 10.1.0.101 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.0.101 255.255.255.0
#
interface Vlan-interface100
 ip address 120.1.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
bgp 100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 10.2.0.101 bfd
 peer 13.1.1.101 as-number 100
 peer 120.1.0.1 as-number 200
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.2.0.101 enable
  peer 10.2.0.101 next-hop-local
  peer 10.2.0.101 route-policy local-pre export
  peer 13.1.1.101 enable
  peer 13.1.1.101 next-hop-local
  peer 120.1.0.1 enable
#
route-policy local-pre permit node 10
 if-match ip address acl 2000
 apply local-preference 200
#
```

```
acl basic 2000
 rule 0 permit source 120.1.0.0 0.0.0.255
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 10.1.0.102 255.255.255.0
#
interface Vlan-interface20
 ip address 10.2.0.102 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

- Device D:

```
#
ospf 1
 import-route direct
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 20
#
vlan 40
#
vlan 100
#
interface Vlan-interface20
ip address 10.2.0.101 255.255.255.0
#
interface Vlan-interface40
 ip address 13.1.1.101 255.255.255.0
#
```

```
interface Vlan-interface100
 ip address 120.1.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
bgp 100
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100
 peer 10.1.0.101 bfd
 peer 120.2.0.1 as-number 300
 peer 192.168.0.101 as-number 100
#
 address-family ipv4 unicast
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local
  peer 10.1.0.101 route-policy local-pre export
  peer 192.168.0.101 enable
  peer 192.168.0.101 next-hop-local
  peer 120.2.0.1 enable
#
acl basic 2000
 rule 0 permit source 120.2.0.0 0.0.0.255
#
```

- Device E:

```
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
vlan 30
#
vlan 40
#
interface Vlan-interface30
 ip address 192.168.0.102 255.255.255.0
#
```

```
interface Vlan-interface40
 ip address 13.1.1.102 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
```

- Device F:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 120.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
bgp 300
 router-id 6.6.6.6
 peer 120.2.0.2 as-number 100
 #
 address-family ipv4 unicast
  network 120.2.0.0 255.255.255.0
  peer 120.2.0.2 enable
#
```

Example: Configuring BFD for PBR

Network configuration

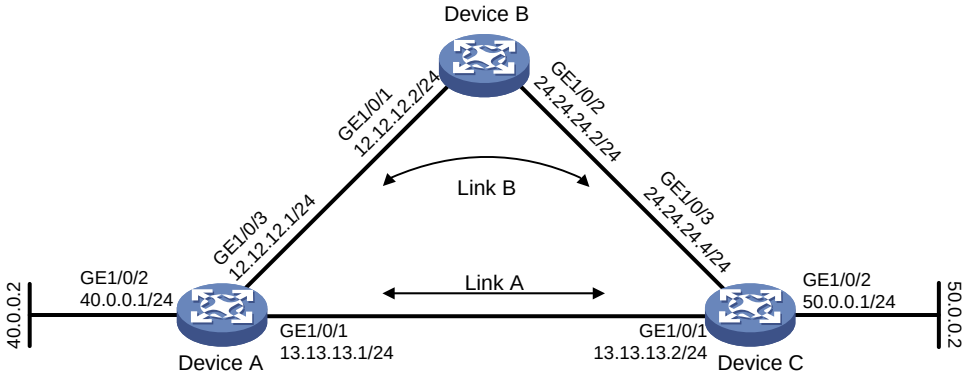
As shown in Figure 7, Device A has two paths to reach Device C:

- Link A.
- Link B.

Configure PBR to enable Device A to forward traffic with source IP address 40.0.0.2 over Link B.

Enable BFD echo packet mode on Device A (Device C does not support BFD) to monitor Link B. When BFD detects a link failure, Device A switches the path to Link A.

Figure 7 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx

WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

The source IP address for BFD echo packets cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Procedures

Configuring interface IP addresses

1. Configure Device A:

```
<DeviceA> system-view
[DeviceA] vlan 40
[DeviceA-vlan40] port gigabitethernet 1/0/2
[DeviceA-vlan40] quit
[DeviceA] interface vlan-interface 40
[DeviceA-Vlan-interface40] ip address 40.0.0.1 24
[DeviceA-Vlan-interface40] quit
```

2. Configure other devices in the same way Device A is configured. (Details not shown.)

Configuring static routes

1. Configure Device A:

   # Configure a static route to reach network 50.0.0.0.

```
[DeviceA] ip route-static 50.0.0.0 24 vlan-interface 200 13.13.13.2
```

2. Configure Device B:

   # Configure a static route to reach network 50.0.0.0.

```
[DeviceB] ip route-static 50.0.0.0 24 vlan-interface 101 24.24.24.4
```

Configuring routing policies on Device A

Create ACL 3010 to permit packets sourced from 40.0.0.2.

```
[DeviceA] acl number 3010
[DeviceA-acl-adv-3010] rule 0 permit ip source 40.0.0.2 0
[DeviceA-acl-adv-3010] quit
```

Create routing policy **aaa** to set next hop 12.12.12.2 for packets matching ACL 3010, and associate the next hop with track entry 11.

```
[DeviceA] policy-based-route aaa permit node 5
[DeviceA-pbr-aaa-5] if-match acl 3010
[DeviceA-pbr-aaa-5] apply next-hop 12.12.12.2 track 11
[DeviceA-pbr-aaa-5] quit
```

Apply routing policy **aaa** to VLAN-interface 40.

```
[DeviceA] interface vlan-interface 40
[DeviceA-Vlan-interface40] ip policy-based-route aaa
[DeviceA-Vlan-interface40] quit
```

Configuring BFD parameters on Device A

Configure the source IP address for BFD echo packets.

```
[DeviceA] bfd echo-source-ip 3.3.3.3
```

Configure the minimum interval for receiving BFD echo packets and the single-hop detection time multiplier, and associate track entry 11 with BFD.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] bfd min-echo-receive-interval 100
[DeviceA-Vlan-interface100] bfd detect-multiplier 3
[DeviceA-Vlan-interface100] quit
[DeviceA] track 11 bfd echo interface vlan-interface100 remote ip 12.12.12.2 local ip
12.12.12.1
[DeviceA-track-11] quit
```

Verifying the configuration

Display outbound traffic statistics for all interfaces on Device A.

```
<DeviceA> reset counters interface
<DeviceA> display counters outbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
GE1/0/1                    0                  0                  0           0
GE1/0/2                    0                  0                  0           0
GE1/0/3               585414                  0                  0           0
GE1/0/4                    0                  0                  0           0
GE1/0/5                    0                  0                  0           0
GE1/0/6                    0                  0                  0           0
```

The output shows that the traffic sourced from 40.0.0.0 is forwarded through VLAN-interface 100 (Link B).

Display BFD session information on Device A.

```
[DeviceA] display bfd session verbose
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:
       Local Discr: 2049
         Source IP: 12.12.12.1         Destination IP: 12.12.12.2
     Session State: Up                      Interface: Vlan-interface100
         Hold Time: 0ms                  Act Tx Inter: 100ms
```

```
      Min Rx Inter: 100ms                Detect Inter: 300ms
          Rx Count: 128234                   Tx Count: 371950
      Connect Type: Direct             Running Up for: 00:01:04
       Detect Mode: Async                        Slot: 1
          Protocol: TRACK
           Version: 1
         Diag Info: No Diagnostic
```

The output shows that a BFD session has been established and is up.

When the link between Device A and Device B fails, view BFD log information.

```
%Dec 10 16:39:46:210 2013 DeviceA BFD/5/BFD_CHANGE_FSM: Sess[12.12.12.1/12.12.12.2,
LD/RD:2049/2049, Interface:Vlan100, SessType:Echo, LinkType:INET], Ver: 1, Sta: UP->
DOWN, Diag: 1 (Control Detection Time Expired)
%Dec 10 16:39:47:343 2013 DeviceA IFNET/5/LINK_UPDOWN: Line protocol on the interface
GigabitEthernet1/0/3 is down.
%Dec 10 16:39:47:343 2013 DeviceA IFNET/3/PHY_UPDOWN: Vlan-interface100 link status
is down.
```

The output shows that the BFD session is down.

Clear the interface statistics, and display outbound traffic statistics for all interfaces on Device A again.

```
<DeviceA> reset counters interface
<DeviceA> display counters outbound interface
Interface         Total (pkts)   Broadcast (pkts)   Multicast (pkts)  Err (pkts)
GE1/0/1                863764                  0                  0           0
GE1/0/2                     0                  0                  0           0
GE1/0/3                     0                  0                  0           0
GE1/0/4                     0                  0                  0           0
GE1/0/5                     0                  0                  0           0
GE1/0/6                     0                  0                  0           0
```

The output shows that the traffic sourced from 40.0.0.0 is forwarded through VLAN-interface 200 (Link A).

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 bfd echo-source-ip 3.3.3.3
#
vlan 40
#
vlan 100
#
vlan 200
#
policy-based-route aaa permit node 5
 if-match acl 3010
```

```
 apply next-hop 12.12.12.2 track 11
#
interface Vlan-interface40
 ip address 40.0.0.1 255.255.255.0
 ip policy-based-route aaa
#
interface Vlan-interface100
 ip address 12.12.12.1 255.255.255.0
 bfd min-echo-receive-interval 100
 bfd detect-multiplier 3
#
interface Vlan-interface200
 ip address 13.13.13.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
 ip route-static 50.0.0.0 24 Vlan-interface200 13.13.13.2
#
 ip local policy-based-route aaa
#
acl number 3010
 rule 0 permit ip source 40.0.0.2 0
#
 track 11 bfd echo interface Vlan-interface100 remote ip 12.12.12.2 local ip 12.
12.12.1
#
```

- Device B:

```
#
vlan 100 to 101
#
interface NULL0
#
interface Vlan-interface100
 ip address 12.12.12.2 255.255.255.0
#
interface Vlan-interface101
 ip address 24.24.24.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 101
#
 ip route-static 50.0.0.0 24 Vlan-interface101 24.24.24.4
```

- Device C:

```
#
vlan 50
#
vlan 101
#
vlan 200
#
interface NULL0
#
interface Vlan-interface50
 ip address 50.0.0.1 255.255.255.0
#
interface Vlan-interface101
 ip address 24.24.24.4 255.255.255.0
#
interface Vlan-interface200
 ip address 13.13.13.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 50
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 101
#
```

Contents

Introduction

This document provides NTP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

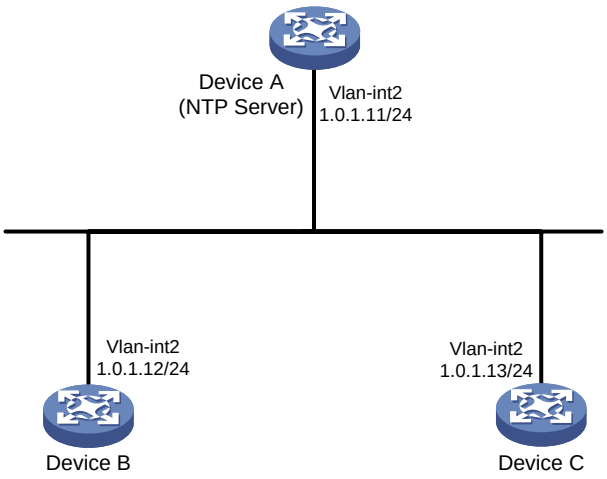
This document assumes that you have basic knowledge of NTP.

Example: Configuring the NTP client/server mode

Network configuration

As shown in Figure 1, configure the NTP client/server mode so all devices can be synchronized to Device A, the NTP server.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx

S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch serie (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device A

Assign an IP address to VLAN-interface 2.

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ip address 1.0.1.11 24
```

```
[DeviceA-Vlan-interface2] quit
```

Enable the NTP service.

```
[DeviceA] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceA] ntp-service refclock-master 2
```

Configuring Device B

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Specify Device A as the NTP server of Device B so that Device B is synchronized to Device A.

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

Configuring Device C

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Specify Device A as the NTP server of Device C so that Device C is synchronized to Device A.

```
[DeviceC] ntp-service unicast-server 1.0.1.11
```

Verifying the configuration

Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.003479 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 1.95313 ms
 Root dispersion: 28.38135 ms
 Reference time: d5ed8cd5.577006ea  Wed, Sep 25 2019 16:24:53.341
 System poll interval: 64 s
```

Verify that an IPv4 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service sessions
        source          reference       stra reach poll  now offset  delay disper
**************************************************************************
```

```
[12345]1.0.1.11        127.127.1.0        2   255   64   38 -10.22 1.9531 3.3416
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A:

```
#
interface Vlan-interface2
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B:

```
#
interface Vlan-interface2
 ip address 1.0.1.12 255.255.255.0
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

- Device C:

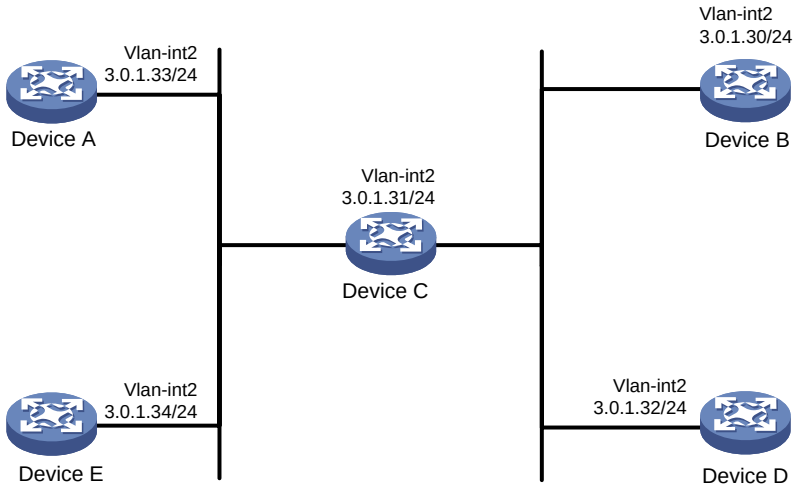
```
#
interface Vlan-interface2
 ip address 1.0.1.13 255.255.255.0
#
 ntp-service enable
 ntp-service unicast-server 1.0.1.11
#
```

Example: Configuring the NTP broadcast mode

Network configuration

As shown in Figure 2, configure the NTP broadcast mode so all devices on the same network segment can be synchronized to Device C, the NTP server.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
S6520-SI switch series	6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device C

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceC] ntp-service refclock-master 2
```

Assign an IP address to VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ip address 3.0.1.31 24
```

Configure Device C to operate in broadcast server mode and send broadcast messages from VLAN-interface 2.

```
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

Configuring Device A, Device B, Device D, and Device E

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

Configure Device A to operate in broadcast client mode and receive broadcast messages on VLAN-interface 2.

```
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

Configure Device B, Device D, and Device E in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Verify that Device A has synchronized to Device C, and the clock stratum level is 3 on Device A and 2 on Device C.

```
[DeviceA-Vlan-interface2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00000 ms
 Root dispersion: 7951.43127 ms
 Reference time: d5ee8d88.2faabed0  Thu, Sep 26 2019 10:40:08.186
 System poll interval: 64 s
```

Verify that an IPv4 NTP association has been established between Device A and Device C.

```
[DeviceA-Vlan-interface2] display ntp-service sessions
      source          reference       stra reach poll  now offset  delay disper
**********************************************************************************
 [1234]3.0.1.31        127.127.1.0        2   254   64   82 -2.190 0.0000 7937.5
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device C:

```
#
interface Vlan-interface2
 ip address 3.0.1.31 255.255.255.0
 ntp-service broadcast-server
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device A:

```
#
```

```
interface Vlan-interface2
 ip address 3.0.1.33 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
#
```

- Device B:

```
#
interface Vlan-interface2
 ip address 3.0.1.30 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
#
```

- Device D:

```
#
interface Vlan-interface2
 ip address 3.0.1.32 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
#
```

- Device E:

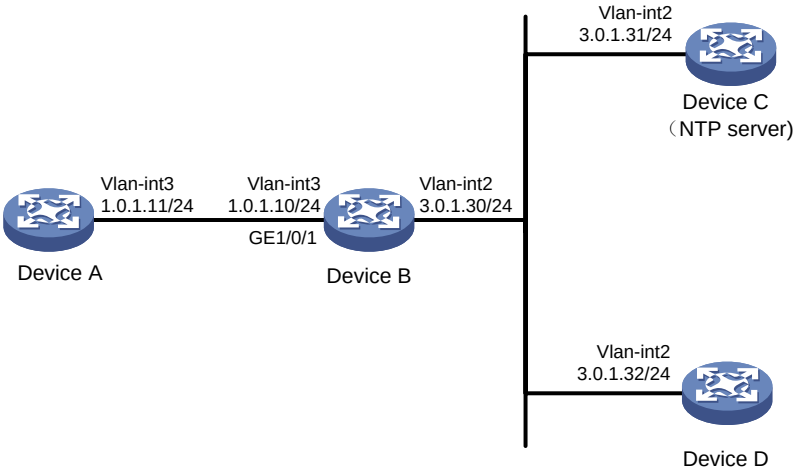
```
#
interface Vlan-interface2
 ip address 3.0.1.34 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
#
```

Example: Configuring the NTP multicast mode

Network configuration

As shown in Figure 3, configure the NTP multicast mode so all devices on different network segments can be synchronized to Device C, the NTP server.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
S6520-SI switch series	6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series	Release 63xx

Hardware	Software version
MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device C

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceC] ntp-service refclock-master 2
```

Assign an IP address to VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ip address 3.0.1.31 24
```

Configure Device C to operate in multicast server mode and send multicast messages from VLAN-interface 2.

```
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

Configuring Device D

Enable the NTP service.

```
<DeviceD> system-view
[DeviceD] ntp-service enable
```

Assign an IP address to VLAN-interface 2.

```
[DeviceD] interface Vlan-interface 2
[DeviceD-Vlan-interface2] ip address 3.0.1.32 24
```

Configure Device D to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
[DeviceD-Vlan-interface2] ntp-service multicast-client
```

Configuring Device B

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Configure Device B to operate in multicast client mode and receive multicast messages on VLAN-interface 2.

```
[DeviceB-Vlan-interface2] ntp-service multicast-client
[DeviceB-Vlan-interface2] quit
```

Because Device A and Device C are on different subnets, you must enable the multicast functions on Device B before Device A can receive multicast messages from Device C.

Enable IP multicast routing and IGMP.

```
[DeviceB] multicast routing
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] pim dm
[DeviceB-Vlan-interface2] quit
[DeviceB] vlan 3
[DeviceB-vlan3] port GigabitEthernet 1/0/1
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] ip address 1.0.1.10 24
[DeviceB-Vlan-interface3] igmp enable
[DeviceB-Vlan-interface3] igmp static-group 224.0.1.1
[DeviceB-Vlan-interface3] quit
[DeviceB] igmp-snooping
[DeviceB-igmp-snooping] quit
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

Configuring Device A

Enable the NTP service.

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

Assign an IP address to VLAN-interface 3.

```
[DeviceA] interface Vlan-interface 3
[DeviceA-Vlan-interface3] ip address 1.0.1.11 24
```

Configure Device A to operate in multicast client mode and receive multicast messages on VLAN-interface 3.

```
[DeviceA-Vlan-interface3] ntp-service multicast-client
```

Verifying the configuration

Verify that Device A has synchronized to Device C, and the clock stratum level is 3 on Device A and 2 on Device C.

```
[DeviceA-Vlan-interface3] display ntp-service status
```

```
Clock status: synchronized
Clock stratum: 3
System peer: 3.0.1.31
Local mode: bclient
Reference clock ID: 3.0.1.31
Leap indicator: 00
Clock jitter: 0.000061 s
Stability: 0.000 pps
Clock precision: 2^-19
Root delay: 1.69373 ms
Root dispersion: 1950.18005 ms
Reference time: d5ee9b15.2f3a684d  Thu, Sep 26 2019 11:37:57.184
System poll interval: 64 s
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A:

```
#
 ntp-service enable
#
interface Vlan-interface3
 ip address 1.0.1.11 255.255.255.0
 ntp-service multicast-client
#
```

- Device B:

```
#
ntp-service enable
#
multicast routing
#
igmp-snooping
#
interface Vlan-interface2
 ip address 3.0.1.30 255.255.255.0
 pim dm
 ntp-service multicast-client
#
interface Vlan-interface3
 ip address 1.0.1.10 255.255.255.0
 igmp enable
```

```
 igmp static-group 224.0.1.1
#
interface GigabitEthernet1/0/1
 port access vlan 3
 igmp-snooping static-group 224.0.1.1 vlan 3
#
```

- Device C:

```
#
 ntp-service enable
ntp-service refclock-master 2
#
interface Vlan-interface2
 ip address 3.0.1.31 255.255.255.0
 ntp-service multicast-server
#
```

- Device D:

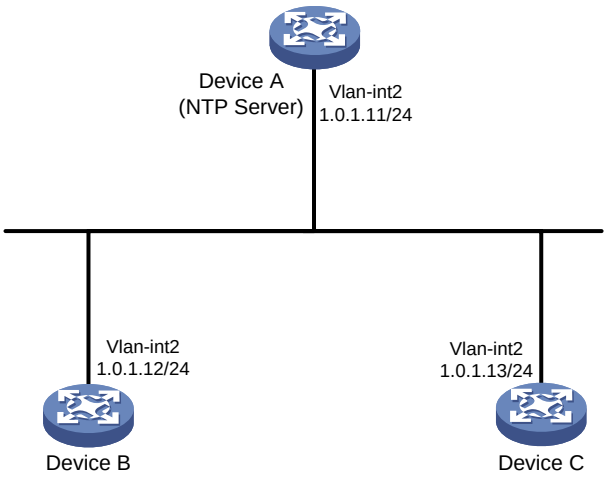
```
#
 ntp-service enable
#
interface Vlan-interface2
 ip address 3.0.1.32 255.255.255.0
 ntp-service multicast-client
#
```

Example: Configuring NTP client/server mode with authentication

Network configuration

As shown in Figure 4, configure the NTP client/server mode so all devices can be synchronized to Device A, the NTP server. Configure NTP authentication on Device A, Device B, and Device C.

Figure 4 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device A

Assign an IP address to VLAN-interface 2.

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ip address 1.0.1.11 24
```

Enable the NTP service.

```
[DeviceA] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceA] ntp-service refclock-master 2
```

Enable NTP authentication on Device A.

```
[DeviceA] ntp-service authentication enable
```

Set an authentication key, and input the key in plain text.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

Specify the key as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

Configuring Device B

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Enable NTP authentication on Device B.

```
[DeviceB] ntp-service authentication enable
```

Set an authentication key, and input the key in plain text.

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

Specify the key as a trusted key.

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Specify Device A as the NTP server of Device B, and associate the server with key 42.

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Configuring Device C

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Enable NTP authentication on Device C.

```
[DeviceC] ntp-service authentication enable
```

Set an authentication key, and input the key in plain text.

```
[DeviceC] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

Specify the key as a trusted key.

```
[DeviceC] ntp-service reliable authentication-keyid 42
```

Specify Device A as the NTP server of Device C, and associate the server with key 42.

```
[DeviceC] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Verifying the configuration

Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Mon, Sep 30 2019 16:06:26.764
 System poll interval: 64 s
```

Verify that an IPv4 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
 [1245]1.0.1.11        127.127.1.0        2     1   64  519   -0.0 0.0065    0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions : 1
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A:

```
#
interface Vlan-interface2
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
```

```
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$4j3SKCgQWBK3Un41B9U0JXzJX9i7IuNoSqi
 ntp-service reliable authentication-keyid 42
 ntp-service refclock-master 2
#
```

- Device B:

```
#
interface Vlan-interface2
 ip address 1.0.1.12 255.255.255.0
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$22eIc8l796cpudZqiaAZ2SLzIfrgzFTVYn8X
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

- Device C:

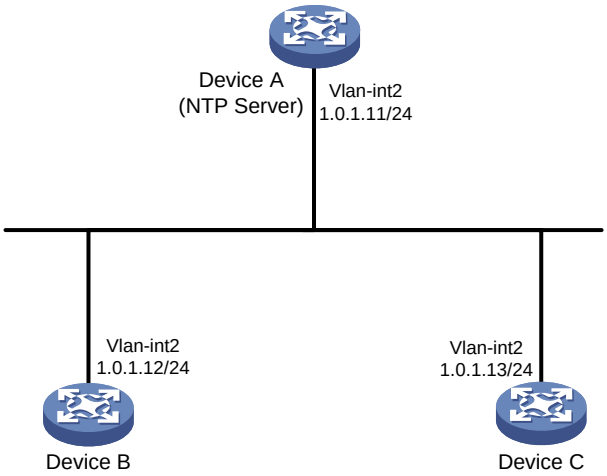
```
#
interface Vlan-interface2
 ip address 1.0.1.13 255.255.255.0
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 42 authentication-mode md5 cipher
$c$3$XJzVmJ1TJbWyYAXpPXxF7JiEOZag8CehibM8
 ntp-service reliable authentication-keyid 42
 ntp-service unicast-server 1.0.1.11 authentication-keyid 42
#
```

Example: Configuring SNTP

Network configuration

As shown in Figure 5, configure SNTP so all devices can be synchronized to Device A, the NTP server.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
S6520-SI switch series	6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device A

Assign an IP address to VLAN-interface 2.

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ip address 1.0.1.11 24
```

Enable the NTP service.

```
[DeviceA] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceA] ntp-service refclock-master 2
```

Configuring Device B

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the SNTP service.

```
<DeviceB> system-view
[DeviceB] sntp enable
```

Specify Device A as the NTP server for Device B.

```
[DeviceB] sntp unicast-server 1.0.1.11
```

Configuring Device C

Assign an IP address to VLAN-interface 2. (Details not shown.)

Enable the SNTP service.

```
<DeviceC> system-view
```

```
[DeviceC] sntp enable
```

Specify Device A as the NTP server for Device C.

```
[DeviceC] sntp unicast-server 1.0.1.11
```

Verifying the configuration

Verify that an SNTP association has been established between Device B and Device A, and Device B has synchronized to Device A.

```
[DeviceB] display sntp sessions
SNTP server     Stratum   Version    Last receive time
1.0.1.11        2         4          Thu, Sep 26 2019 17:25:09.121 (Synced)
```

Configuration files

- Device A:

```
#
interface Vlan-interface2
 ip address 1.0.1.11 255.255.255.0
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B:

```
#
interface Vlan-interface2
 ip address 1.0.1.12 255.255.255.0
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

- Device C:

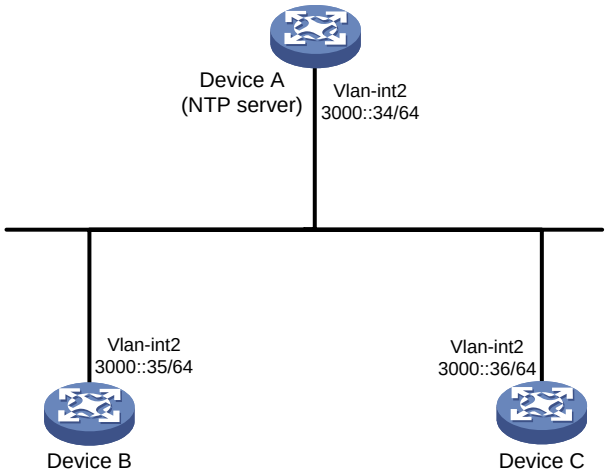
```
#
interface Vlan-interface2
 ip address 1.0.1.13 255.255.255.0
#
 sntp enable
 sntp unicast-server 1.0.1.11
#
```

Example: Configuring the IPv6 NTP client/server mode

Network configuration

As shown in Figure 1, configure the IPv6 NTP client/server mode so all devices can synchronize to Device A, the NTP server.

Figure 6 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx

Hardware	Software version
S6520-SI switch series	
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series	Release 63xx

Hardware	Software version
MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device A

Assign an IPv6 address to VLAN-interface 2.

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ipv6 address 3000::34 64
[DeviceA-Vlan-interface2] quit
```

Enable the NTP service.

```
[DeviceA] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceA] ntp-service refclock-master 2
```

Configuring Device B

Assign an IPv6 address to each interface. (Details not shown.)

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Specify Device A as the NTP server of Device B so that Device B is synchronized to Device A.

```
[DeviceB] ntp-service unicast-server 3000::34
```

Configuring Device C

Assign an IPv6 address to each interface. (Details not shown.)

Enable the NTP service.

```
<DeviceC> system-view
```

```
[DeviceC] ntp-service enable
```

Specify Device A as the NTP server of Device C so that Device C is synchronized to Device A.

```
[DeviceC] ntp-service unicast-server 3000::34
```

Verifying the configuration

Verify that Device B has synchronized to Device A, and the clock stratum level is 3 on Device B and 2 on Device A.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::34
 Local mode: client
 Reference clock ID: 95.197.17.40
 Leap indicator: 00
 Clock jitter: 0.003479 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 1.95313 ms
 Root dispersion: 28.38135 ms
 Reference time: d5ed8cd5.577006ea  Wed, Sep 25 2019 16:24:53.341
 System poll interval: 64 s
```

Verify that an IPv6 NTP association has been established between Device B and Device A.

```
[DeviceB] display ntp-service ipv6 sessions
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.

 Source: [12345] 3000::34
 Reference: 127.127.1.0          Clock stratum: 2
 Reachabilities: 3               Poll interval: 64
 Last receive time: 62           Offset: 0.1272
 Roundtrip delay: 1.8158         Dispersion: 188.47

 Total sessions: 1
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A:

```
#
interface Vlan-interface2
```

```
 ipv6 address 3000::34/64
#
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B:

```
#
interface Vlan-interface2
 ipv6 address 3000::35/64
#
 ntp-service enable
 ntp-service ipv6 unicast-server 3000::34
#
```

- Device C:

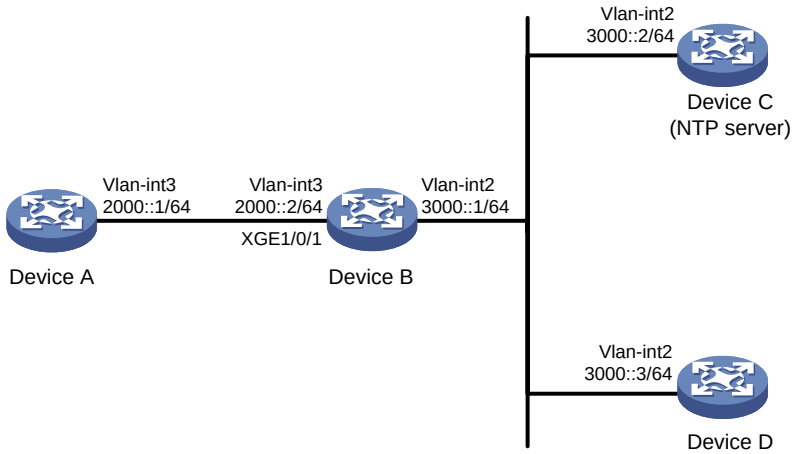
```
#
interface Vlan-interface2
 ipv6 address 3000::36/64
#
 ntp-service enable
 ntp-service ipv6 unicast-server 3000::34
#
```

Example: Configuring the IPv6 NTP multicast mode

Network configuration

As shown in Figure 3, configure the IPv6 NTP multicast mode so all devices on different network segments can synchronize to Device C, the NTP server.

Figure 7 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configuring Device C

Configure routing protocols so that all devices can reach each other. (Details not shown.)

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2.

```
[DeviceC] ntp-service refclock-master 2
```

Assign an IPv6 address to VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ipv6 address 3000::2 64
```

Configure Device C to operate in IPv6 multicast server mode and send multicast messages from VLAN-interface 2.

```
[DeviceC-Vlan-interface2] ntp-service ipv6 multicast-server ff24::1
[DeviceC-Vlan-interface2] quit
```

Configuring Device D

Configure routing protocols and assign an IP address to each interface so that all devices can reach each other. (Details not shown.)

Enable the NTP service.

```
<DeviceD> system-view
[DeviceD] ntp-service enable
```

Configure Device D to operate in IPv6 multicast client mode and receive multicast messages on VLAN-interface 2.

```
[DeviceD-Vlan-interface2] ntp-service ipv6 multicast-client ff24::1
[DeviceD-Vlan-interface2] quit
```

Configuring Device B

Configure routing protocols and assign an IP address to each interface so that all devices can reach each other. (Details not shown.)

Enable the NTP service.

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

Configure Device B to operate in IPv6 multicast client mode and receive multicast messages on VLAN-interface 2.

```
[DeviceB-Vlan-interface2] ntp-service ipv6 multicast-client ff24::1
[DeviceB-Vlan-interface2] quit
```

Because Device A and Device C are on different subnets, you must enable IPv6 multicast functions on Device B before Device A can receive multicast messages from Device C.

Enable IPv6 multicast functions.

```
[DeviceB] ipv6 multicast routing
[DeviceB-mrib6] quit
```

```
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ipv6 pim dm
[DeviceB-Vlan-interface2] quit
[DeviceB] vlan 3
[DeviceB-vlan3] port GigabitEthernet 1/0/1
[DeviceB-vlan3] quit
[DeviceB] interface vlan-interface 3
[DeviceB-Vlan-interface3] mld enable
[DeviceB-Vlan-interface3] mld static-group ff24::1
[DeviceB-Vlan-interface3] quit
[DeviceB] mld-snooping
[DeviceB-mld-snooping] quit
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] mld-snooping static-group ff24::1 vlan 3
[DeviceB-mld-snooping] quit
```

Configuring Device A

Configure routing protocols and assign an IP address to each interface so that all devices can reach each other. (Details not shown.)

Enable the NTP service.

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

Configure Device A to operate in IPv6 multicast client mode and receive multicast messages on VLAN-interface 3.

```
[DeviceA-Vlan-interface3] ntp-service ipv6 multicast-client ff24::1
[DeviceA-Vlan-interface3] quit
```

Verifying the configuration

Verify that Device A has synchronized to Device C, and the clock stratum level is 3 on Device A and 2 on Device C.

```
[DeviceA] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3000::2
 Local mode: bclient
 Reference clock ID: 165.84.121.65
 Leap indicator: 00
 Clock jitter: 0.000061 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 1.69373 ms
 Root dispersion: 1950.18005 ms
 Reference time: d5ee9b15.2f3a684d  Thu, Sep 26 2019 11:37:57.184
 System poll interval: 64 s
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A:

```
#
 ntp-service enable
#
interface Vlan-interface3
 ipv6 address 2000::1/64
 ntp-service ipv6 multicast-client ff24::1
#
```

- Device B:

```
#
ntp-service enable
#
ipv6 multicast routing
#
mld-snooping
#
interface Vlan-interface2
 ipv6 address 3000::1/64
 ipv6 pim dm
 ntp-service ipv6 multicast-client ff24::1
#
interface Vlan-interface3
 ipv6 address 2000::2/64
 mld enable
 mld static-group ff24::1
#
interface GigabitEthernet1/0/1
 port access vlan 3
 mld-snooping static-group ff24::1 vlan 3
#
```

- Device C:

```
#
 ntp-service enable
ntp-service refclock-master 2
#
interface Vlan-interface2
 ipv6 address 3000::2/64
 ntp-service ipv6 multicast-server ff24::1
```

```
#
```

- Device D:

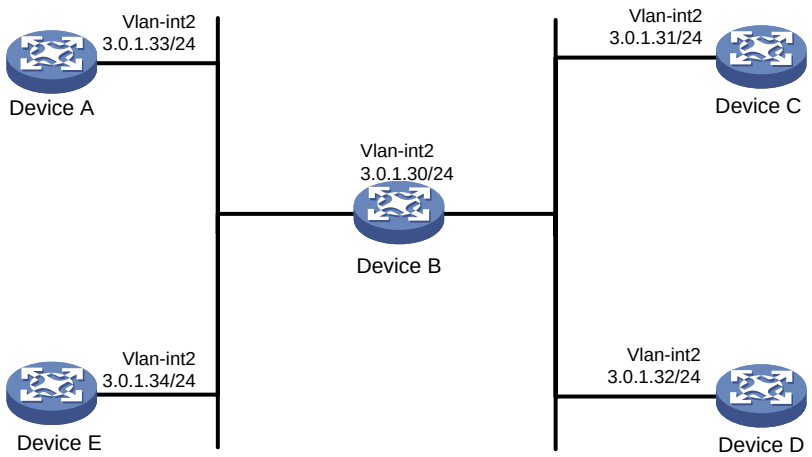
```
#
 ntp-service enable
#
interface Vlan-interface2
 ipv6 address 3000::3/64
 ntp-service ipv6 multicast-client ff24::1
#
```

Example: Configuring NTP broadcast mode with authentication

Network configuration

As shown in Figure 4, configure NTP broadcast mode so all devices can synchronize to Device A, the NTP server. Configure NTP authentication on Device A, Device B, and Device C.

Figure 8 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx

Hardware	Software version
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx

Hardware	Software version
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C E152C E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Release 6810 and later versions

Procedures

Configure Device C

Enable the NTP service.

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

Specify the local clock as the reference source, with the stratum level 2 on Device C.

```
[DeviceC] ntp-service refclock-master 2
```

Enable NTP authentication on Device C. Configure an NTP authentication key, with the key ID of **88** and key value of **123456**. Input the key in plain text, and specify it as a trusted key.

```
[DeviceC] ntp-service authentication enable
[DeviceC] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[DeviceC] ntp-service reliable authentication-keyid 88
```

Specify Device C as an NTP broadcast server, and associate key **88** with Device C.

```
[DeviceC] interface vlan-interface 2
[DeviceC-Vlan-interface2] ip address 3.0.1.31 24
[DeviceC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
[DeviceC-Vlan-interface2] quit
```

Configure Device A

Enable the NTP service.

```
<DeviceA> system-view
[DeviceA] ntp-service enable
```

Enable NTP authentication on Device A. Configure an NTP authentication key, with the key ID of **88** and key value of **123456**. Input the key in plain text, and specify it as a trusted key.

```
[DeviceA] ntp-service authentication enable
[DeviceA] ntp-service authentication-keyid 88 authentication-mode md5 simple 123456
[DeviceA] ntp-service reliable authentication-keyid 88
```

Configure Device A to operate in NTP broadcast client mode and receive NTP broadcast messages on VLAN-interface 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
[DeviceA-Vlan-interface2] ip address 3.0.1.33 24
[DeviceA-Vlan-interface2] quit
```

Configure Device B, Device D, and Device E in the same way Device A is configured. (Details not shown.)

Verifying the configuration

Verify that Device A has synchronized to Device C, and the clock stratum level is 3 on Device A and 2 on Device C.

```
[DeviceA] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: bclient
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000092 s
 Stability: 0.000 pps
 Clock precision: 2^-19
 Root delay: 2.42615 ms
 Root dispersion: 1950.98877 ms
 Reference time: d5eed631.2f498d71  Thu, Sep 26 2019 15:50:09.184
 System poll interval: 64 s
```

NOTE:

- For the S6550XE-HI switch series and the S6525XE-HI switch series, the value is 2^-21 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S6812 switch series, S6813 switch series, and S5850 switch series, the value is 2^-23 for the **Clock precision** field in the output from the **`display ntp-service status`** command.
- For the S5170-EI switch series and S5570S-EI switch series, the value is 2^-18 for the **Clock precision** field in the output from the **`display ntp-service status`** command.

Configuration files

- Device A, Device B, Device D, and Device E:

```
#
interface Vlan-interface2
 ip address 3.0.1.33 255.255.255.0
 ntp-service broadcast-client
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher
$c$3$pU6KvpS80MadhM2zM
CCSR07HX4qEbJhHvQ==
 ntp-service reliable authentication-keyid 88
#
```

- Device C:

```
#
interface Vlan-interface2
 ip address 3.0.1.31 255.255.255.0
 ntp-service broadcast-server authentication-keyid 88
#
 ntp-service enable
 ntp-service authentication enable
 ntp-service authentication-keyid 88 authentication-mode md5 cipher
$c$3$iJudDKiqCVO+gOaG53
63/fz4M3dQvHo2Fw==
 ntp-service reliable authentication-keyid 88
 ntp-service refclock-master 3
#
```

Contents

Introduction

This document provides SNMP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

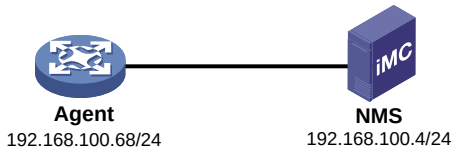
This document assumes that you have basic knowledge of SNMP.

Example: Configuring SNMPv1 or SNMPv2c

Network configuration

As shown in Figure 1, an IMC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv1/SNMPv2c to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx

Hardware	Software version
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	IE4520
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure SNMPv1 or SNMPv2c, follow these restrictions and guidelines:

- The configuration procedure is the same for SNMPv1 and SNMPv2c. This example uses SNMPv2c.
- For the NMS to manage the SNMP agent, the SNMP settings on the agent and the NMS must match.
- The NMS software configuration varies by vendor. This example uses the IMC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.

Procedures

Configuring the SNMP agent

Specify SNMPv2c, and create read-only community **readtest** and read and write community **writetest**.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

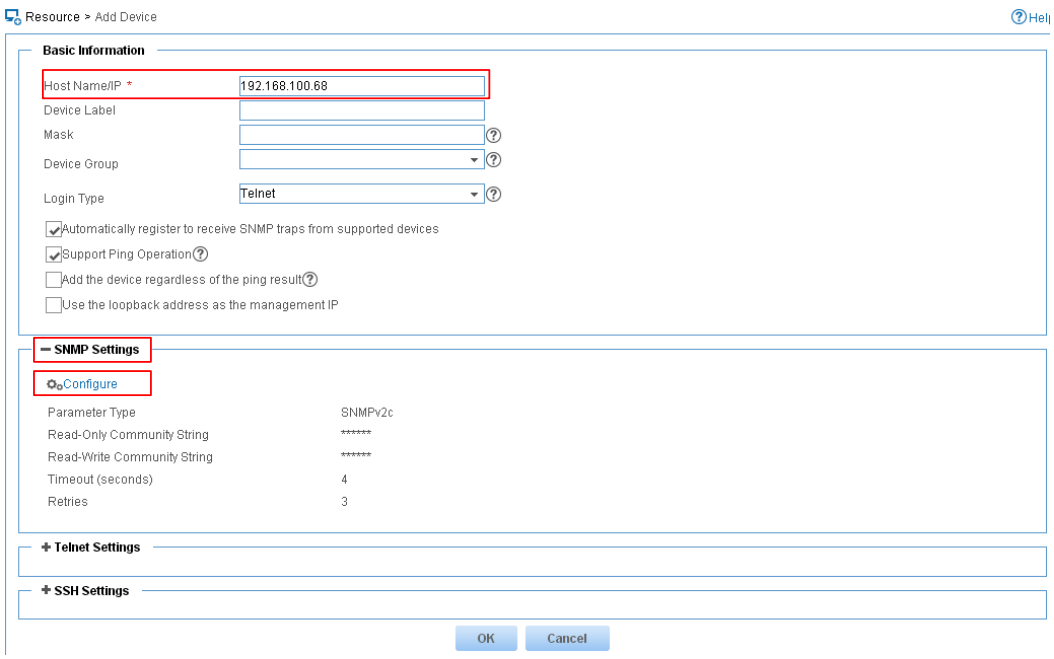
Enable SNMP notifications, specify the NMS at 192.168.100.4 as the SNMP trap destination, and use **readtest** as the community name.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
readtest v2c
```

Configuring the NMS

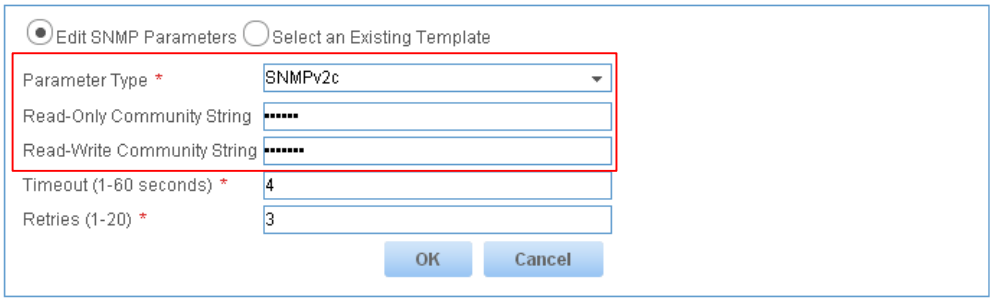
1. Add the device (SNMP agent) to the IMC:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Resource Management** > **Add Device**.
   c. On the **Add Device** page, configure the following parameters:
      – Enter **192.168.100.68** in the **Host Name/IP** field.
      – Use the default values for other parameters.

Figure 2 Adding a device



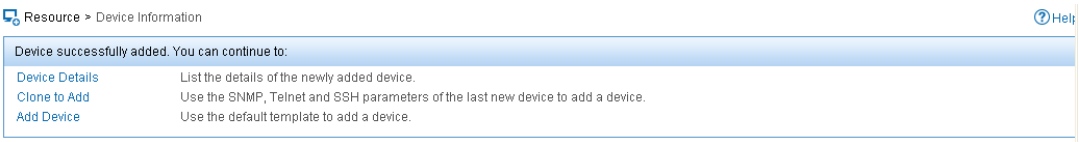
2. Configure SNMP parameters:
   a. Expand the **SNMP Settings** area.
   b. Click **Configure**.
   c. On the page that appears, configure the following parameters:
      – Select **SNMPv2c** from the **Parameter Type** list.
      – Enter **readtest** in the **Read-Only Community String** field.
      – Enter **writetest** in the **Read-Write Community String** field.
      – Use the default values for other parameters.
      – Click **OK**.

   Figure 3 Configuring SNMP parameters



3. On the **Add Device** page, click **OK**.
   The device is successfully added to the IMC, as shown in Figure 4.

   Figure 4 Device added



Verifying the configuration

1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
   a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
   b. Click the **Alarm** tab.
   c. From the navigation tree, select **Alarm Browse** > **All Alarms**.

Configuration files

```
#
 snmp-agent
 snmp-agent community write writetest
 snmp-agent community read readtest
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v2c
```

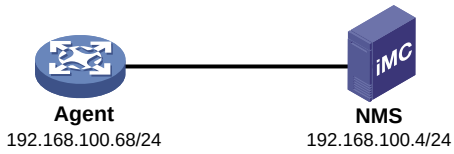
```
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityn
ame readtest v2c
#
```

Example: Configuring SNMPv3

Network configuration

As shown in Figure 5, an IMC server acts as the NMS and the device acts as the agent. The NMS uses SNMPv3 to manage the SNMP agent, and the agent automatically sends notifications to report events to the NMS.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Release 8005 and later versions, and Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release

Hardware	Software version
	6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx

Hardware	Software version
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 series	IE4520
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

When you configure SNMPv3, follow these restrictions and guidelines:

- SNMPv3 supports VACM and RBAC access control modes. This example provides SNMPv3 configuration procedures in both modes. See "Configuring the SNMP agent in RBAC mode" and "Configuring the SNMP agent in VACM mode"..
- For the NMS to manage the SNMP agent, the SNMP settings on the agent and the NMS must match.
- The NMS software configuration varies by vendor. This example uses the IMC PLAT 7.0 (E0202). For information about configuring the NMS, see the NMS manual.
- For the NMS to receive notifications from the agent, make sure the following configurations are the same on the NMS and the SNMP agent:
  - SNMPv3 username.
  - SNMP protocol version.
  - Authentication algorithm.
  - Privacy algorithm.
  - Authentication and privacy keys.

Procedures

Configuring the SNMP agent in RBAC mode

Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

Create user role **test**, and assign **test** read and write access to the objects under the **internet** subtree (OID: 1.3.6.1).

```
[Agent] role name test
[Agent-role-test] rule 1 permit read write oid 1.3.6.1
[Agent-role-test] quit
```

Create SNMPv3 user **managev3user**. Assign user role **test** to **managev3user.** Set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encyption key to **123456TESTencr&!**.

```
[Agent] snmp-agent usm-user v3 managev3user user-role test simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

Specify the NMS at **192.168.100.4** as the trap destination, and set the username to **managev3user** for the traps.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

Configuring the SNMP agent in VACM mode

Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

Include the **mib-2** (OID 1.3.6.1) subtree in the **mibtest** view.

```
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```

Create SNMPv3 group **managev3group**, and specify the authentication with privacy security model for the group. Assign the group read, write, and notification accesses to the **mibtest** view.

```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest
notify-view mibtest
```

Add user **managev3user** to SNMPv3 group **managev3group**, and set the authentication algorithm to **sha**, authentication key to **123456TESTauth&!**, encryption algorithm to **aes128**, and encryption key to **123456TESTencr&!.**

```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha
123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

Configure contact and physical location information for the agent.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

Enable SNMP notifications.

```
[Agent] snmp-agent trap enable
```

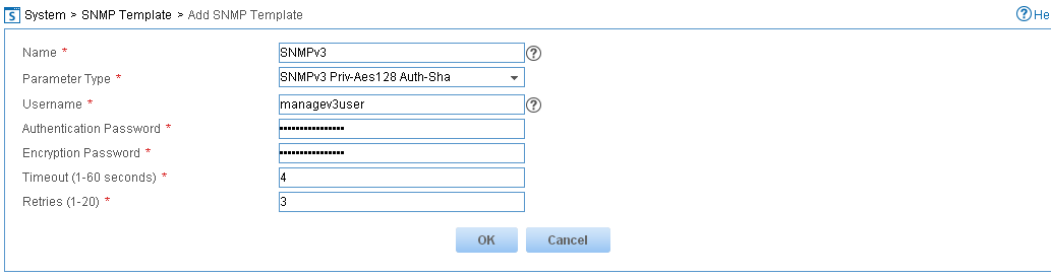
Specify the NMS at **192.168.100.4** as the trap destination, and set the username to **managev3user** for the traps.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

Configuring the NMS

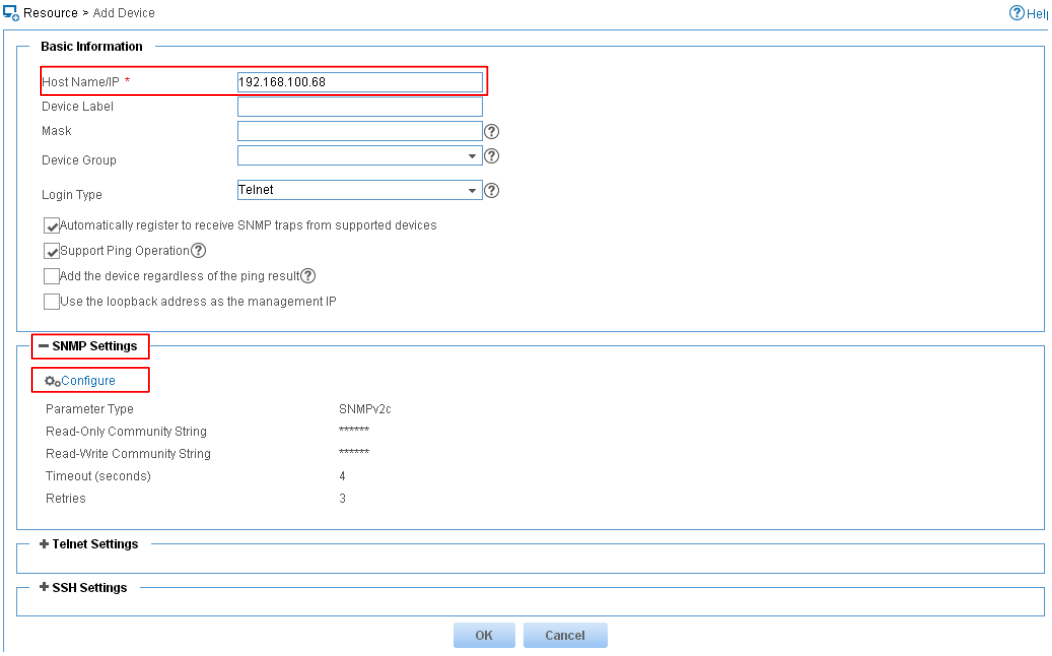
1. Add an SNMP template:
   a. Click the **System** tab.
   b. From the navigation tree, select **Resource Management** > **SNMP Template**.
   c. On the **SNMP Template** page, click **Add**.
   d. On the **Add SNMP Template** page, configure the following parameters:
      – Enter **SNMPv3** in the **Name** field.
      – Select **SNMPv3 Priv-Aes128 Auth-Sha** from the **Parameter Type** list.
      – Enter **managev3user** in the **Username** field.
      – Enter **123456TESTauth&!** in the **Authentication Password** field.
      – Enter **123456TESTencr&!** in the **Encryption Password** field.
      – Use the default values for other parameters.
      – Click **OK**.

Figure 6 Adding an SNMP template



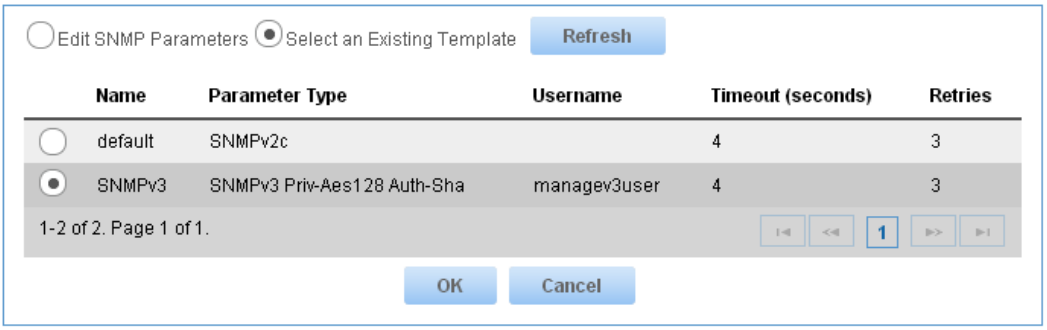
2. Add the device (SNMP agent) to IMC:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Resource Management** > **Add Device**.
   c. On the **Add Device** page, configure the following parameters:
      – Enter **192.168.100.68** in the **Host Name/IP** field.
      – Use the default values for other parameters.

Figure 7 Adding a device



3. Configure SNMP parameters:
   a. Expand the **SNMP Settings** area.
   b. Click **Configure**.
   c. Select the **Select an Existing Template** option.
   d. Select template name **SNMPv3**.
   e. Click **OK**.

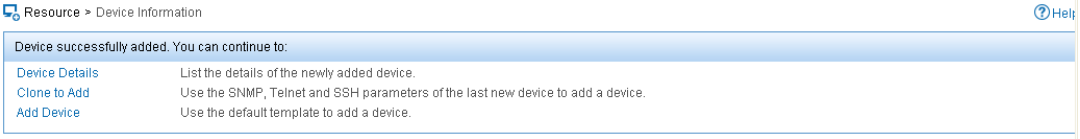
Figure 8 Selecting an existing template



4. On the **Add Device** page, click **OK**.

   The device is successfully added to IMC, as shown in Figure 9.

Figure 9 Device added



Verifying the configuration

1. Verify that the agent sends notifications to the NMS when the link state of an interface changes:
   a. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
   b. Click the **Alarm** tab.
   c. From the navigation tree, select **Alarm Browse** > **All Alarms**.

Configuration files

SNMPv3 configuration in RBAC mode

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user user-role test cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
role name test
 rule 1 permit read oid 1.3.6.1
#
```

SNMPv3 configuration in VACM mode

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest
notify-view mibtest
 snmp-agent mib-view included mibtest internet
 snmp-agent trap enable arp
 snmp-agent trap enable syslog

 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
```

Contents

Introduction

This document provides NQA configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of NQA.

General restrictions and guidelines

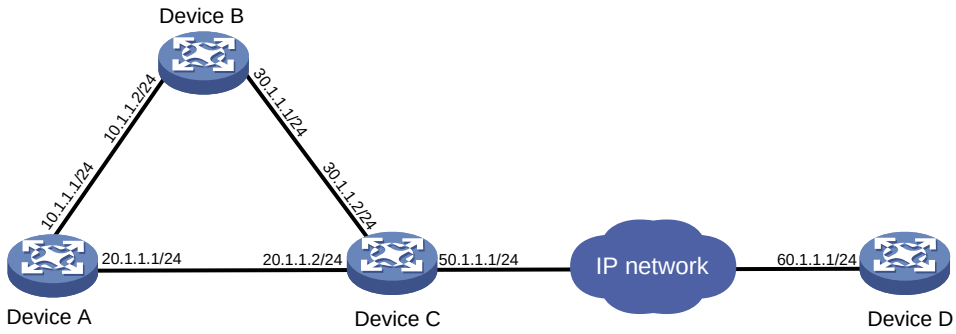
The ICMP echo operation is not supported in IPv6 networks. To test the reachability of an IPv6 address, use the **`ping ipv6`** command.

Example: Configuring an NQA ICMP echo operation

Network configuration

As shown in Figure 1, configure an NQA ICMP echo operation to test the roundtrip time between Device A and Device D through Device B.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA ICMP echo operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create an NQA ICMP echo operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type icmp-echo
```

Specify the destination IP address of ICMP echo requests as 60.1.1.1.

```
[DeviceA-nqa-admin-test-icmp-echo] destination ip 60.1.1.1
```

Specify the next hop of ICMP echo requests as 10.1.1.2.

```
[DeviceA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```

Configure the ICMP echo operation to perform 10 probes.

```
[DeviceA-nqa-admin-test-icmp-echo] probe count 10
```

Specify the probe timeout time as 500 milliseconds for the ICMP echo operation.

```
[DeviceA-nqa-admin-test-icmp-echo] probe timeout 500
```

Configure the ICMP echo operation to repeat at an interval of 5000 milliseconds.

```
[DeviceA-nqa-admin-test-icmp-echo] frequency 5000
```

Enable saving history records.

```
[DeviceA-nqa-admin-test-icmp-echo] history-record enable
```

Configure the maximum number of history records that can be saved as 10.

```
[DeviceA-nqa-admin-test-icmp-echo] history-record number 10
[DeviceA-nqa-admin-test-icmp-echo] quit
```

Verifying the configuration

Start the ICMP echo operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the ICMP echo operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the ICMP echo operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2019-03-23 15:00:01.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the ICMP echo operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2019-03-23 15:00:01.2
```

```
  369         3             Succeeded         2019-03-23 15:00:01.2
  368         3             Succeeded         2019-03-23 15:00:01.2
  367         5             Succeeded         2019-03-23 15:00:01.2
  366         3             Succeeded         2019-03-23 15:00:01.2
  365         3             Succeeded         2019-03-23 15:00:01.2
  364         3             Succeeded         2019-03-23 15:00:01.1
  363         2             Succeeded         2019-03-23 15:00:01.1
  362         3             Succeeded         2019-03-23 15:00:01.1
  361         2             Succeeded         2019-03-23 15:00:01.1
```

The output shows that the packets sent by Device A can reach Device D through Device B. No packet loss occurs during the operation. The minimum, maximum, and average round-trip times are 2, 5, and 3 milliseconds, respectively.

Configuration files

```
#
nqa entry admin test
 type icmp-echo
  destination ip 60.1.1.1
  frequency 5000
  history-record enable
  history-record number 10
  next-hop ip 10.1.1.2
  probe count 10
  probe timeout 500
#
```

Example: Configuring an NQA ICMP jitter operation

Network configuration

As shown in Figure 1, configure an ICMP jitter operation to test the jitter between Device A and Device B.

Figure 2 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA ICMP jitter operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create an NQA ICMP jitter operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type icmp-jitter
```

Specify 10.2.2.2 as the destination address for the operation.

```
[DeviceA-nqa-admin-test-icmp-jitter] destination ip 10.2.2.2
```

Configure the operation to repeat every 1000 milliseconds.

```
[DeviceA-nqa-admin-test-icmp-jitter] frequency 1000
[DeviceA-nqa-admin-test-icmp-jitter] quit
```

Verifying the configuration

Start the ICMP jitter operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the ICMP jitter operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the ICMP jitter operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 13
    Last packet received time: 2019-03-09 17:40:29.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 10
    Min positive SD: 0                   Min positive DS: 0
    Max positive SD: 0                   Max positive DS: 0
    Positive SD number: 0                Positive DS number: 0
    Positive SD sum: 0                   Positive DS sum: 0
    Positive SD average: 0               Positive DS average: 0
    Positive SD square-sum: 0            Positive DS square-sum: 0
    Min negative SD: 1                   Min negative DS: 2
    Max negative SD: 1                   Max negative DS: 2
    Negative SD number: 1                Negative DS number: 1
    Negative SD sum: 1                   Negative DS sum: 2
    Negative SD average: 1               Negative DS average: 2
    Negative SD square-sum: 1            Negative DS square-sum: 4
```

```
  One way results:
    Max SD delay: 1                         Max DS delay: 2
    Min SD delay: 1                         Min DS delay: 2
    Number of SD delay: 1                   Number of DS delay: 1
    Sum of SD delay: 1                      Sum of DS delay: 2
    Square-Sum of SD delay: 1               Square-Sum of DS delay: 4
    Lost packets for unknown reason: 0
```

Display the statistics of the ICMP jitter operation.

```
[DeviceA] display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2019-03-09 17:42:10.7
    Life time: 156 seconds
    Send operation times: 1560           Receive response times: 1560
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 1563
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 1560
    Min positive SD: 1                      Min positive DS: 1
    Max positive SD: 1                      Max positive DS: 2
    Positive SD number: 18                  Positive DS number: 46
    Positive SD sum: 18                     Positive DS sum: 49
    Positive SD average: 1                  Positive DS average: 1
    Positive SD square-sum: 18              Positive DS square-sum: 55
    Min negative SD: 1                      Min negative DS: 1
    Max negative SD: 1                      Max negative DS: 2
    Negative SD number: 24                  Negative DS number: 57
    Negative SD sum: 24                     Negative DS sum: 58
    Negative SD average: 1                  Negative DS average: 1
    Negative SD square-sum: 24              Negative DS square-sum: 60
  One way results:
    Max SD delay: 1                         Max DS delay: 2
    Min SD delay: 1                         Min DS delay: 1
    Number of SD delay: 4                   Number of DS delay: 4
    Sum of SD delay: 4                      Sum of DS delay: 5
    Square-Sum of SD delay: 4               Square-Sum of DS delay: 7
Lost packets for unknown reason: 0
```

Configuration files

```
#
```

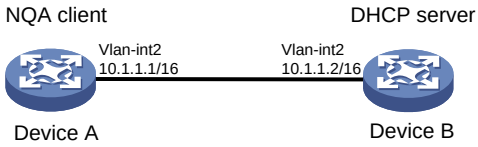
```
nqa entry admin test
 type icmp-jitter
  destination ip 10.2.2.2
  frequency 1000
#
```

Example: Configuring an NQA DHCP operation

Network configuration

As shown in Figure 3, configure an NQA DHCP operation to test the time required for Device A to obtain an IP address from the DHCP server (Device B).

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx

ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx

E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA DHCP operation, follow these restrictions and guidelines:

- Complete the DHCP server configuration before you start the DHCP operation.
- Make sure the devices can reach each other before you start the operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create an NQA DHCP operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dhcp
```

Specify the DHCP server IP address 10.1.1.2 as the destination address.

```
[DeviceA-nqa-admin-test-dhcp] destination ip 10.1.1.2
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dhcp] history-record enable
[DeviceA-nqa-admin-test-dhcp] quit
```

Verifying the configuration

Start the DHCP operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the DHCP operation.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 624/624/624
      Square-Sum of round trip time: 389376
      Last succeeded probe time: 2020-03-24 09:56:03.2
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the DHCP operation.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          624          Succeeded        2019-03-24 09:56:03.2
```

The output shows that it took Device A 624 milliseconds to obtain an IP address from the DHCP server.

Configuration files

```
#
nqa entry admin test
 type dhcp
  destination ip 10.1.1.2
  history-record enable
#
```

Example: Configuring an NQA DNS operation

Network configuration

As shown in Figure 4, configure an NQA DNS operation to test whether Device A can perform address resolution through the DNS server and test the resolution time.

Figure 4 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA DNS operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create an NQA DNS operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dns
```

Specify the IP address of the DNS server 10.2.2.2 as the destination address.

```
[DeviceA-nqa-admin-test-dns] destination ip 10.2.2.2
```

Specify the domain name to be translated as **host.com**.

```
[DeviceA-nqa-admin-test-dns] resolve-target host.com
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dns] history-record enable
[DeviceA-nqa-admin-test-dns] quit
```

Verifying the configuration

Start the DNS operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the DNS operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the DNS operation.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 62/62/62
      Square-Sum of round trip time: 3844
      Last succeeded probe time: 2020-03-24 10:49:37.3
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the DNS operation.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          62           Succeeded        2019-03-24 10:49:37.3
```

The output shows that it took Device A 62 milliseconds to translate the domain name **host.com** into an IP address.

Configuration files

```
#
nqa entry admin test
 type dns
  destination ip 10.2.2.2
  history-record enable
  resolve-target host.com
#
```

Example: Configuring an NQA FTP operation

Network configuration

As shown in Figure 5, configure an NQA FTP operation to test the file transmission time between Device A and the FTP server. The login username and password are **admin** and **systemtest**, respectively.

Figure 5 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx,

	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series	Release 63xx

S5000V5-EI switch series	
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA FTP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.
- When you perform the **put** operation with the **`filename`** command configured, make sure the file exists on the NQA client.
- Take the network bandwidth into consideration when you set the file size and the probe timeout.

Procedures

Create an NQA FTP operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type ftp
```

Specify the URL of the FTP server.

```
[DeviceA-nqa-admin-test-ftp] url ftp://10.2.2.2
```

Specify 10.1.1.1 as the source IP address.

```
[DeviceA-nqa-admin-test-ftp] source ip 10.1.1.1
```

Specify the FTP operation type as **put**.

```
[DeviceA-nqa-admin-test-ftp] operation put
```

Specify the file to be uploaded as **config.txt**.

```
[DeviceA-nqa-admin-test-ftp] filename config.txt
```

Specify the username for the FTP operation as **admin**.

```
[DeviceA-nqa-admin-test-ftp] username admin
```

Specify the password for the FTP operation as **systemtest**.

```
[DeviceA-nqa-admin-test-ftp] password simple systemtest
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-ftp] history-record enable
[DeviceA-nqa-admin-test-ftp] quit
```

Verifying the configuration

Start the FTP operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the FTP operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the FTP operation.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 173/173/173
      Square-Sum of round trip time: 29929
      Last succeeded probe time: 2019-03-25 10:07:28.6
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the FTP operation.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1           173          Succeeded        2019-03-25 10:07:28.6
```

The output shows that it took Device A 173 milliseconds to upload a file to the FTP server.

Configuration files

```
#
nqa entry admin test
 type ftp
  filename config.txt
  history-record enable
```

```
  operation put
  password cipher $c$3$BP255atzDilAfIPwfh+RMHqmP5LTiKWpVf/hpBs=
  source ip 10.1.1.1
  url ftp://10.2.2.2
  username admin
#
```

Example: Configuring an NQA HTTP operation

Network configuration

As shown in Figure 6, configure an NQA HTTP operation on the NQA client to test the time required to obtain data from the HTTP server.

Figure 6 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx

E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA HTTP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create an NQA HTTP operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type http
```

Specify the URL of the HTTP server.

```
[DeviceA-nqa-admin-test-http] url http://10.2.2.2/index.htm
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-http] history-record enable
[DeviceA-nqa-admin-test-http] quit
```

Verifying the configuration

Start the HTTP operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the HTTP operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the HTTP operation.

```
[DeviceA] display nqa result admin test
  NQA entry(admin admin, tag test) test results:
      Send operation times: 1              Receive response times: 1
      Min/Max/Average round trip time: 64/64/64
      Square-Sum of round trip time: 4096
      Last succeeded probe time: 2019-03-25 11:12:47.9
    Extend results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
```

Display the history records of the HTTP operation.

```
[DeviceA] display nqa history admin test
  NQA entry(admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1          64           Succeeded        2019-03-25 11:12:47.9
```

The output shows that it took Device A 64 milliseconds to obtain data from the HTTP server.

Configuration files

```
#
nqa entry admin test
 type http
  history-record enable
  url http://10.2.2.2/index.htm
#
```

Example: Configuring an NQA UDP jitter operation

Network configuration

As shown in Figure 7, configure a UDP jitter operation to test the jitter, delay, and round-trip time between Device A and Device B.

Figure 7 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4300V2 switch series MS4320V3 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA UDP jitter operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the NQA server before you start the NQA UDP jitter operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Configuring Device B

Enable the NQA server.

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

Configure a listening service to listen on the IP address 10.2.2.2 and UDP port 9000.

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

Configuring Device A

Create a UDP jitter operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-jitter
```

Configure 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[DeviceA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-jitter] destination port 9000
```

Configure the operation to repeat at an interval of 1000 milliseconds.

```
[DeviceA-nqa-admin-test-udp-jitter] frequency 1000
[DeviceA-nqa-admin-test-udp-jitter] quit
```

Verifying the configuration

Start the UDP jitter operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the UDP jitter operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the UDP jitter operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 10             Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
    Last packet received time: 2019-07-30 09:46:36.9
  Extended results:
    Packet loss ratio: 0%
```

```
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 10
    Min positive SD: 1                    Min positive DS: 0
    Max positive SD: 1                    Max positive DS: 0
    Positive SD number: 1                 Positive DS number: 0
    Positive SD sum: 1                    Positive DS sum: 0
    Positive SD average: 1                Positive DS average: 0
    Positive SD square-sum: 1             Positive DS square-sum: 0
    Min negative SD: 0                    Min negative DS: 0
    Max negative SD: 0                    Max negative DS: 0
    Negative SD number: 0                 Negative DS number: 0
    Negative SD sum: 0                    Negative DS sum: 0
    Negative SD average: 0                Negative DS average: 0
    Negative SD square-sum: 0             Negative DS square-sum: 0
  One way results:
    Max SD delay: 0                       Max DS delay: 0
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 0                 Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
```

Display the statistics of the UDP jitter operation.

```
[DeviceA] display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2019-07-30 09:46:22.7
    Life time: 14 seconds
    Send operation times: 150             Receive response times: 150
    Min/Max/Average round trip time: 1/4/1
    Square-Sum of round trip time: 165
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 150
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 6                    Max positive DS: 1
    Positive SD number: 11                Positive DS number: 5
```

```
  Positive SD sum: 16                  Positive DS sum: 5
  Positive SD average: 1               Positive DS average: 1
  Positive SD square-sum: 46           Positive DS square-sum: 5
  Min negative SD: 5                   Min negative DS: 1
  Max negative SD: 5                   Max negative DS: 1
  Negative SD number: 1                Negative DS number: 1
  Negative SD sum: 5                   Negative DS sum: 1
  Negative SD average: 5               Negative DS average: 1
  Negative SD square-sum: 25           Negative DS square-sum: 1
One way results:
  Max SD delay: 0                      Max DS delay: 0
  Min SD delay: 0                      Min DS delay: 0
  Number of SD delay: 0                Number of DS delay: 0
  Sum of SD delay: 0                   Sum of DS delay: 0
  Square-Sum of SD delay: 0            Square-Sum of DS delay: 0
  SD lost packets: 0                   DS lost packets: 0
  Lost packets for unknown reason: 0
```

Configuration files

- Device B:

```
#
 nqa server enable
 nqa server udp-echo 10.2.2.2 9000
#
```

- Device A:

```
#
nqa entry admin test
 type udp-jitter
  destination ip 10.2.2.2
  destination port 9000
  frequency 1000
#
```

Example: Configuring an NQA SNMP operation

Network configuration

As shown in Figure 8, configure an SNMP operation to test the time the NQA client uses to get a response from the SNMP agent.

Figure 8 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA SNMP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the SNMP agent before you start the NQA SNMP operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Configuring Device B

Set the SNMP version to **all**.

```
<DeviceB> system-view
[DeviceB] snmp-agent sys-info version all
```

Set the read community to **public**.

```
[DeviceB] snmp-agent community read public
```

Set the write community to **private**.

```
[DeviceB] snmp-agent community write private
```

Configuring Device A

Create an SNMP operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type snmp
```

Configure 10.2.2.2 as the destination IP address of the SNMP operation.

```
[DeviceA-nqa-admin-test-snmp] destination ip 10.2.2.2
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-snmp] history-record enable
[DeviceA-nqa-admin-test-snmp] quit
```

Verifying the configuration

Start the SNMP operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the SNMP operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the SNMP operation.

```
[DeviceA] display nqa result admin test
```

```
NQA entry (admin admin, tag test) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 1
    Last succeeded probe time: 2019-07-30 10:07:28.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the SNMP operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
Index      Response     Status           Time
1          1            Succeeded        2019-07-30 10:07:28.2
```

Configuration files

- Device B:

  ```
  #
   snmp-agent
   snmp-agent local-engineid 800063A20300E0FC123456
   snmp-agent community read public
   snmp-agent community write private
   snmp-agent sys-info version all
  #
  ```

- Device A:

  ```
  #
  nqa entry admin test
   type snmp
    destination ip 10.2.2.2
    history-record enable
  #
  ```

Example: Configuring an NQA TCP operation

Network configuration

As shown in Figure 9, configure a TCP operation to test the time required for Device A and Device B to establish a TCP connection.

Figure 9 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA TCP operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the NQA server before you start the NQA TCP operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Configuring Device B

Enable the NQA server.

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

Configure a listening service to listen on the IP address 10.2.2.2 and TCP port 9000.

```
[DeviceB] nqa server tcp-connect 10.2.2.2 9000
```

Configuring Device A

Create a TCP operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type tcp
```

Configure 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[DeviceA-nqa-admin-test-tcp] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-tcp] destination port 9000
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-tcp] history-record enable
[DeviceA-nqa-admin-test-tcp] quit
```

Verifying the configuration

Start the TCP operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the TCP operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the TCP operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
```

```
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 1
    Last succeeded probe time: 2019-07-30 10:37:29.5
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the TCP operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
Index      Response     Status           Time
2          1            Succeeded        2019-07-30 10:37:29.5
1          0            Unknown error    2019-07-30 10:34:55.9
```

Configuration files

- Device B:

```
#
 nqa server enable
 nqa server tcp-connect 10.2.2.2 9000
#
```

- Device A:

```
#
nqa entry admin test
 type tcp
  destination ip 10.2.2.2
  destination port 9000
  history-record enable
#
```

Example: Configuring an NQA UDP echo operation

Network configuration

As shown in Figure 10, configure a UDP echo operation to test the round-trip time between Device A and Device B. The destination port number is 8000.

Figure 10 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA UDP echo operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the NQA server before you start the NQA UDP echo operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Configuring Device B

Enable the NQA server.

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

Configure a listening service to listen on the IP address 10.2.2.2 and UDP port 8000.

```
[DeviceB] nqa server udp-echo 10.2.2.2 8000
```

Configuring Device A

Create a UDP echo operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type udp-echo
```

Configure 10.2.2.2 as the destination IP address and port 8000 as the destination port.

```
[DeviceA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-udp-echo] destination port 8000
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-udp-echo] history-record enable
[DeviceA-nqa-admin-test-udp-echo] quit
```

Verifying the configuration

Start the UDP echo operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the UDP echo operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the UDP echo operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
```

```
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 1
    Last succeeded probe time: 2019-07-30 11:10:35.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the UDP echo operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history record(s):
Index      Response     Status           Time
1          1            Succeeded        2019-07-30 11:10:35.2
```

Configuration files

- Device B:

```
#
 nqa server enable
 nqa server udp-echo 10.2.2.2 8000
#
```

- Device A:

```
#
nqa entry admin test
 type udp-echo
  destination ip 10.2.2.2
  destination port 8000
  history-record enable
#
```

Example: Configuring an NQA UDP tracert operation

Network configuration

As shown in Figure 11, configure a UDP tracert operation to determine the routing path from Device A to Device B.

Figure 11 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA UDP tracert operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the NQA server before you start the NQA UDP tracert operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

1. Execute the **ip ttl-expires enable** command on the intermediate devices and execute the **ip unreachables enable** command on Device B. (Details not shown.)
2. Configure Device A:

   # Create a UDP tracert operation.

   ```
   <DeviceA> system-view
   [DeviceA] nqa entry admin test
   [DeviceA-nqa-admin-test] type udp-tracert
   ```

   # Specify 10.2.2.2 as the destination IP address for the operation.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] destination ip 10.2.2.2
   ```

   # Set the destination port number to 33434. (This step is optional because it is the default setting.)

   ```
   [DeviceA-nqa-admin-test-udp-tracert] destination port 33434
   ```

   # Configure Device A to perform three probes to each hop.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] probe count 3
   ```

   # Set the probe timeout time to 500 milliseconds.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] probe timeout 500
   ```

   # Configure the UDP tracert operation to repeat every 5000 milliseconds.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] frequency 5000
   ```

   # Specify M-GigabitEthernet 0/0/0 as the output interface for the probe packets.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] out interface m-gigabitethernet0/0/0
   ```

   # Enable the no-fragmentation feature.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] no-fragment enable
   ```

   # Set the maximum number of consecutive probe failures to 6.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] max-failure 6
   ```

   # Set the TTL value to 1 for UDP packets in the start round of the UDP tracert operation.

   ```
   [DeviceA-nqa-admin-test-udp-tracert] init-ttl 1
   ```

Verifying the configuration

Start the UDP tracert operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the UDP tracert operation runs for a period of time, stop the operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

Display the most recent result of the UDP tracert operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
```

```
    Send operation times: 6              Receive response times: 6
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 1
    Last succeeded probe time: 2019-09-09 14:46:06.2
  Extended results:
    Packet loss in test: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
Failures due to other errors: 0
  UDP-tracert results:
    TTL     Hop IP             Time
    1       3.1.1.1            2019-09-09 14:46:03.2
    2       10.2.2.2           2019-09-09 14:46:06.2
```

Display the history records of the UDP tracert operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history records:
Index      TTL  Response  Hop IP           Status          Time
1          2    2         10.2.2.2         Succeeded       2019-09-09 14:46:06.2
1          2    1         10.2.2.2         Succeeded       2019-09-09 14:46:05.2
1          2    2         10.2.2.2         Succeeded       2019-09-09 14:46:04.2
1          1    1         3.1.1.1          Succeeded       2019-09-09 14:46:03.2
1          1    2         3.1.1.1          Succeeded       2019-09-09 14:46:02.2
1          1    1         3.1.1.1          Succeeded       2019-09-09 14:46:01.2
```

Configuration files

```
#
nqa entry admin test
 type udp-tracert
  destination ip 10.2.2.2
  frequency 5000
  max-failure 6
  no-fragment enable
  out interface m-gigabitethernet0/0/0
  probe timeout 500
#
```

Example: Configuring an NQA voice operation

Network configuration

As shown in Figure 12, configure a voice operation to test the jitter, delay, MOS, and ICPIF between Device A and Device B.

Figure 12 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx

S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch	Release 63xx

IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA voice operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- Configure Device B as the NQA server before you start the NQA voice operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Configuring Device B

Enable the NQA server.

```
<DeviceB> system-view
[DeviceB] nqa server enable
```

Configure a listening service to listen on IP address 10.2.2.2 and UDP port 9000.

```
[DeviceB] nqa server udp-echo 10.2.2.2 9000
```

Configuring Device A

Create a voice operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type voice
```

Configure 10.2.2.2 as the destination IP address and port 9000 as the destination port.

```
[DeviceA-nqa-admin-test-voice] destination ip 10.2.2.2
[DeviceA-nqa-admin-test-voice] destination port 9000
[DeviceA-nqa-admin-test-voice] quit
```

Verifying the configuration

Start the voice operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the voice operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the voice operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 157           Receive response times: 157
    Min/Max/Average round trip time: 1/3/1
```

```
    Square-Sum of round trip time: 165
    Last packet received time: 2019-07-30 14:27:52.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 157
    Min positive SD: 2                    Min positive DS: 1
    Max positive SD: 4                    Max positive DS: 1
    Positive SD number: 2                 Positive DS number: 5
    Positive SD sum: 6                    Positive DS sum: 5
    Positive SD average: 3                Positive DS average: 1
    Positive SD square-sum: 20            Positive DS square-sum: 5
    Min negative SD: 2                    Min negative DS: 1
    Max negative SD: 4                    Max negative DS: 1
    Negative SD number: 2                 Negative DS number: 6
    Negative SD sum: 6                    Negative DS sum: 6
    Negative SD average: 3                Negative DS average: 1
    Negative SD square-sum: 20            Negative DS square-sum: 6
  One way results:
    Max SD delay: 0                       Max DS delay: 0
    Min SD delay: 0                       Min DS delay: 0
    Number of SD delay: 0                 Number of DS delay: 0
    Sum of SD delay: 0                    Sum of DS delay: 0
    Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
    SD lost packets: 0                    DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    MOS value: 0.00                       ICPIF value: 0
```

Display the statistics of the voice operation.

```
[DeviceA] display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2019-07-30 14:30:30.0
    Life time: 204 seconds
    Send operation times: 4000           Receive response times: 4000
    Min/Max/Average round trip time: 1/32/1
    Square-Sum of round trip time: 12853
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
```

```
  Packets arrived late: 0
Voice results:
 RTT number: 4000
  Min positive SD: 1                    Min positive DS: 1
  Max positive SD: 32                   Max positive DS: 1
  Positive SD number: 76                Positive DS number: 72
  Positive SD sum: 567                  Positive DS sum: 72
  Positive SD average: 7                Positive DS average: 1
  Positive SD square-sum: 9011          Positive DS square-sum: 72
  Min negative SD: 1                    Min negative DS: 1
  Max negative SD: 20                   Max negative DS: 1
  Negative SD number: 87                Negative DS number: 67
  Negative SD sum: 569                  Negative DS sum: 67
  Negative SD average: 7                Negative DS average: 1
  Negative SD square-sum: 6715          Negative DS square-sum: 67
One way results:
  Max SD delay: 0                       Max DS delay: 0
  Min SD delay: 0                       Min DS delay: 0
  Number of SD delay: 0                 Number of DS delay: 0
  Sum of SD delay: 0                    Sum of DS delay: 0
  Square-Sum of SD delay: 0             Square-Sum of DS delay: 0
  SD lost packets: 0                    DS lost packets: 0
  Lost packets for unknown reason: 0
Voice scores:
  Max MOS value: 4.40                   Min MOS value: 4.40
   Max ICPIF value: 0                    Min ICPIF value: 0
```

Configuration files

- Device B:

```
#
 nqa server enable
 nqa server udp-echo 10.2.2.2 8000
#
```

- Device A:

```
#
nqa entry admin test
 type voice
  destination ip 10.2.2.2
  destination port 9000
#
```

Example: Configuring an NQA DLSw operation

Network configuration

As shown in Figure 13, configure a DLSw operation to test the response time of the DLSw device.

Figure 13 Network diagram

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

S6520-SI switch series	
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series	Release 63xx

MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA DLSw operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

Create a DLSw operation.

```
<DeviceA> system-view
[DeviceA] nqa entry admin test
[DeviceA-nqa-admin-test] type dlsw
```

Configure 10.2.2.2 as the destination IP address.

```
[DeviceA-nqa-admin-test-dlsw] destination ip 10.2.2.2
```

Enable the saving of history records.

```
[DeviceA-nqa-admin-test-dlsw] history-record enable
[DeviceA-nqa-admin-test-dlsw] quit
```

Verifying the configuration

Start the DLSw operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the DLSw operation runs for a time period, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the DLSw operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2019-07-22 10:40:27.7
```

```
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

Display the history records of the DLSw operation.

```
[DeviceA] display nqa history admin test
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  1          19           Succeeded        2019-07-22 10:40:27.7
```

Configuration files

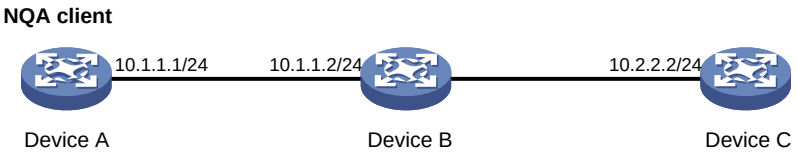
```
#
nqa entry admin test
 type dlsw
  destination ip 10.2.2.2
  history-record enable
#
```

Example: Configuring an NQA path jitter operation

Network configuration

As shown in Figure 14, configure a path jitter operation to test the round trip time and jitters from Device A to Device B and Device C.

Figure 14 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure an NQA path jitter operation, follow these restrictions and guidelines:

- Make sure the devices can reach each other before you start the NQA operation.
- You cannot modify the operation configuration for a running NQA operation.

Procedures

1. Execute the **ip ttl-expires enable** command on Device B and execute the **ip unreachables enable** command on Device C. (Details not shown.)
2. Configure Device A:

   # Create a path jitter operation.

   ```
   <DeviceA> system-view
   [DeviceA] nqa entry admin test
   [DeviceA-nqa-admin-test] type path-jitter
   ```

   # Specify 10.2.2.2 as the destination IP address for the operation.

   ```
   [DeviceA-nqa-admin-test-path-jitter] destination ip 10.2.2.2
   ```

   # Configure the path jitter operation to repeat every 10000 milliseconds.

   ```
   [DeviceA-nqa-admin-test-path-jitter] frequency 10000
   [DeviceA-nqa-admin-test-path-jitter] quit
   ```

Verifying the configuration

Start the path jitter operation.

```
[DeviceA] nqa schedule admin test start-time now lifetime forever
```

After the path jitter operation runs for a period of time, stop the operation.

```
[DeviceA] undo nqa schedule admin test
```

Display the most recent result of the path jitter operation.

```
[DeviceA] display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Hop IP 10.1.1.2
    Basic Results
      Send operation times: 10             Receive response times: 10
      Min/Max/Average round trip time: 9/21/14
      Square-Sum of round trip time: 2419
    Extended Results
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results
      Jitter number: 9
        Min/Max/Average jitter: 1/10/4
      Positive jitter number: 6
        Min/Max/Average positive jitter: 1/9/4
        Sum/Square-Sum positive jitter: 25/173
      Negative jitter number: 3
        Min/Max/Average negative jitter: 2/10/6
        Sum/Square-Sum positive jitter: 19/153

  Hop IP 10.2.2.2
    Basic Results
```

```
  Send operation times: 10              Receive response times: 10
  Min/Max/Average round trip time: 15/40/28
  Square-Sum of round trip time: 4493
Extended Results
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
Path-Jitter Results
  Jitter number: 9
    Min/Max/Average jitter: 1/10/4
  Positive jitter number: 6
    Min/Max/Average positive jitter: 1/9/4
    Sum/Square-Sum positive jitter: 25/173
  Negative jitter number: 3
    Min/Max/Average negative jitter: 2/10/6
    Sum/Square-Sum positive jitter: 19/153
```

Configuration files

```
#
nqa entry admin test
 type path-jitter
  destination ip 10.2.2.2
  frequency 10000
#
```

Contents

Introduction

This document provides configuration examples of port mirroring and flow mirroring.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of port mirroring and flow mirroring.

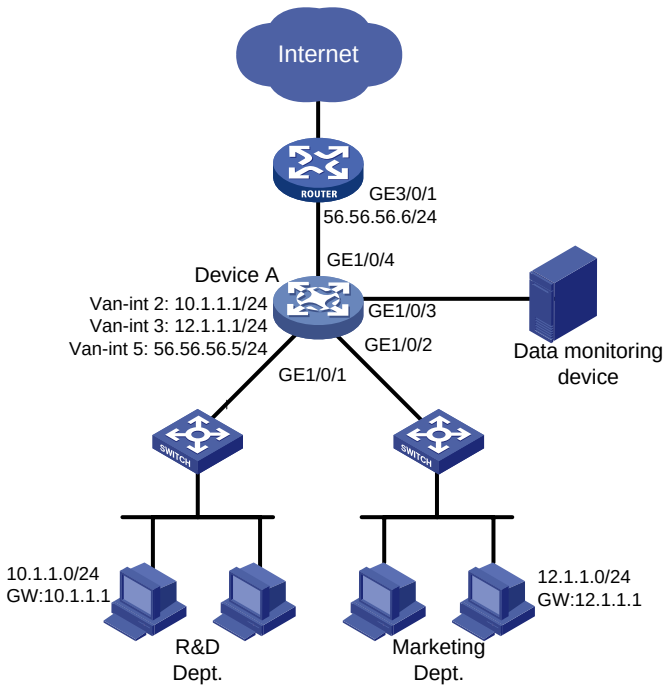
General restrictions and guidelines

Example: Configuring local port mirroring

Network configuration

As shown in Figure 1, configure local port mirroring to monitor the Internet traffic and bidirectional traffic of the Marketing department and the Technical department.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx

Hardware	Software version
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure local port mirroring, follow these restrictions and guidelines:

- A local mirroring group takes effect only when you configure both source ports and the monitor port for the group. When you configure the monitor port, do not use a port of an existing mirroring group.
- Use a monitor port only for port mirroring, so the data monitoring device receives and analyzes only the mirrored traffic.
- For the correct operation of port mirroring, disable the spanning tree feature on the monitor port if it is a Layer 2 interface.

Procedures

Create VLAN 2, VLAN 3, and VLAN 5.

```
<DeviceA> system-view
[DeviceA] vlan 2 3 5
```

Create VLAN-interface 2 and VLAN-interface 3, and assign IP addresses to them separately, which will act as the gateways for VLAN 2 and VLAN 3 separately.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 12.1.1.1 24
[DeviceA-Vlan-interface3] quit
```

Create VLAN-interface 5, and assign IP address 56.56.56.5 to the interface.

```
[DeviceA] interface vlan-interface 5
[DeviceA-Vlan-interface5] ip address 56.56.56.5 24
[DeviceA-Vlan-interface5] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 2, GigabitEthernet 1/0/2 to VLAN 3, and GigabitEthernet 1/0/4 to VLAN 5.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 2
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 3
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port access vlan 5
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 2 and VLAN 3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 2 3
[DeviceA-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as the source ports of the mirroring group.

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2
inbound
```

Configure GigabitEthernet 1/0/3 as the monitor port of the mirroring group.

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Display information about mirroring group 1 on Device A.

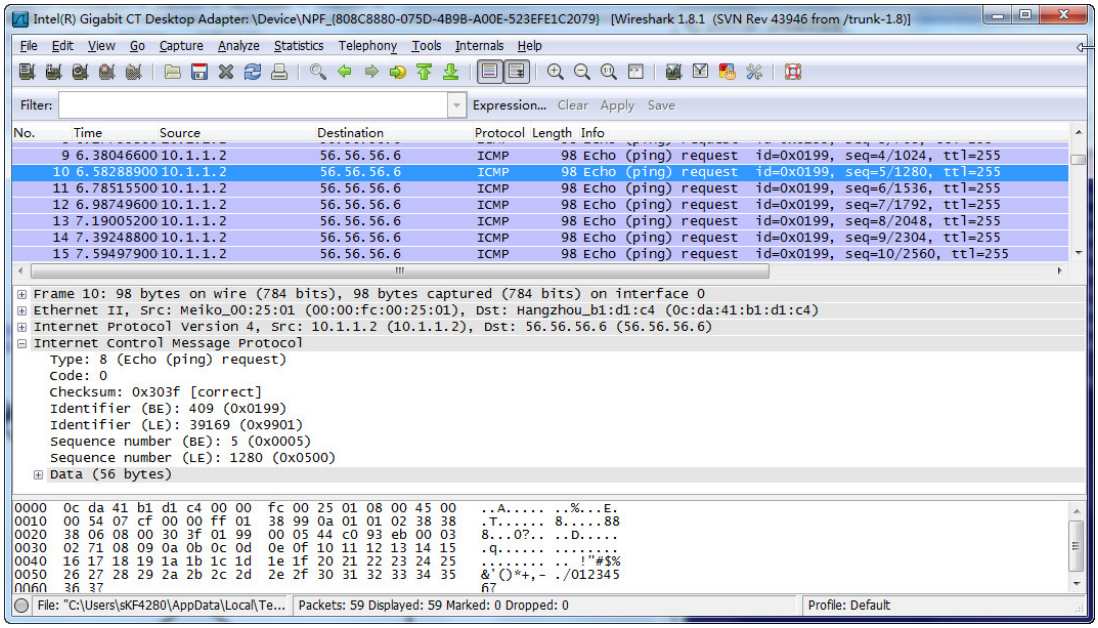
```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
        GigabitEthernet1/0/2  Inbound
    Monitor port: GigabitEthernet1/0/3
```

2. Use Wireshark for packet analysis:

   # Ping 56.56.56.6 from a Technical department host (10.1.1.2). (Details not shown.)

   # Use Wireshark on the data monitoring device to capture the ping packets.

   Figure 2 Ping packet analysis in Wireshark



   The analysis shows that the data monitoring device can monitor the packets sent from the Technical department.

Configuration files

IMPORTANT:

The **`port link-mode`** command is not supported on the following switches:

- S5130S-HI switch series.
- S5130S-EI switch series.
- S5135S-EI switch series.
- S3100V3-EI switch series.
- E128C switch.
- E152C switch.
- E500C switch series.
- E500D switch series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M switch series.
- IE4320 switch series.

```
#
vlan 2
#
vlan 3
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 12.1.1.1 255.255.255.0
#
interface Vlan-interface5
 ip address 56.56.56.5 255.255.255.0
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
```

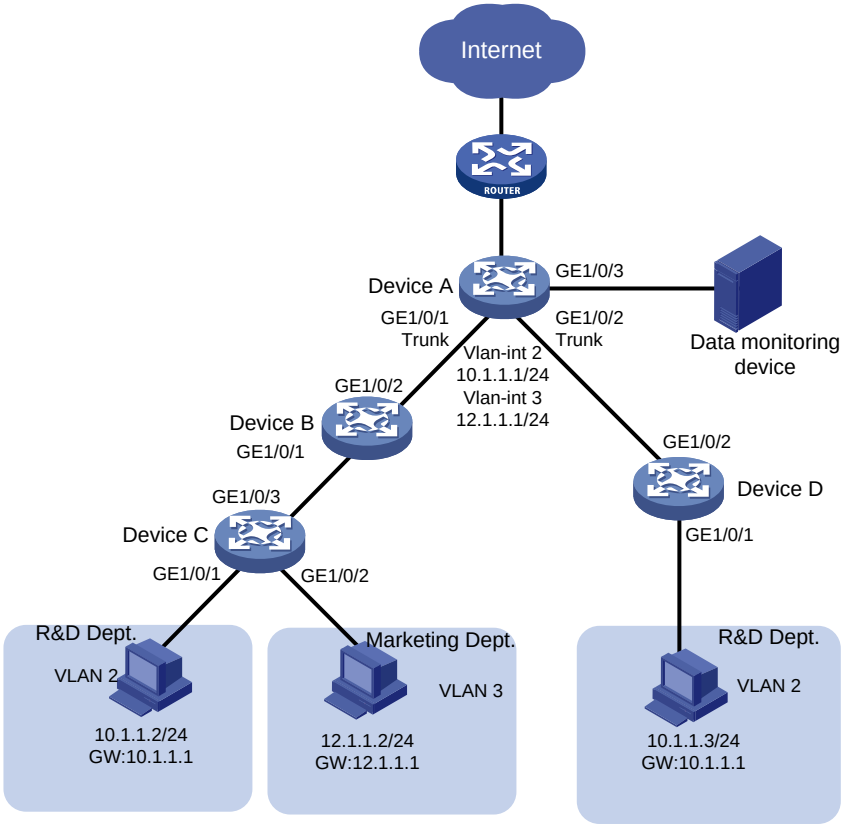
```
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 5
#
```

Example: Configure Layer 2 remote port mirroring

Network configuration

As shown in Figure 3, configure Layer 2 remote port mirroring to monitor the outgoing traffic from the Technical department.

Figure 3 Network diagram



Analysis

To ensure correct forwarding of mirrored packets, assign the ports that connect intermediate devices to the source and destination devices to the remote probe VLAN.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except	Release 11xx

Hardware	Software version
S5500V3-24P-SI and S5500V3-48P-SI)	
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch	Release 63xx

Hardware	Software version
IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure devices for remote port mirroring, configure them in the order of the destination device, the intermediate devices, and the source device.

When you configure the monitor port for the remote destination group on the destination device, follow these restrictions and guidelines:

- Do not use a port of an existing mirroring group.
- Use the monitor port only for port mirroring.
- For the correct operation of port mirroring, disable the spanning tree feature on the monitor port if it is a Layer 2 interface.
- For the monitor port to forward mirrored packets to the data monitoring device without VLAN tags, assign the monitor port to the remote probe VLAN as an access port.

When you configure the remote probe VLAN on the source and destination devices, follow these restrictions and guidelines:

- Use an existing static VLAN that is not in use.
- Use the remote probe VLAN for port mirroring exclusively.
- The remote mirroring groups on the source device and destination device must use the same remote probe VLAN. Use this VLAN only for the same remote mirroring group on the source device and destination device.

When you configure a remote source group on the source device, follow these restrictions and guidelines:

- Do not assign source ports of the remote source group to the remote probe VLAN.
- To ensure the operation of mirroring, do not enable any of the following features on the egress port:
  - Spanning tree.
  - 802.1X.
  - IGMP snooping.
  - Static ARP.
  - MAC address learning.
- A port of an existing mirroring group cannot be configured as an egress port.
- A mirroring group contains only one egress port.
- To implement Layer 2 remote mirroring when the source ports are Layer 3 interfaces, you must use the egress port method.

Procedures

Configuring Device A (the destination device)

Create VLANs 2 and 3.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

Create VLAN-interface 2 and assign an IP address to it.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
```

Create VLAN-interface 3 and assign an IP address to it.

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 12.1.1.1 24
[DeviceA-Vlan-interface3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 2, 3, and 5.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 3 5
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLANs 2 and 5.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 2 5
[DeviceA-GigabitEthernet1/0/2] quit
```

Create a remote destination group.

```
[DeviceA] mirroring-group 1 remote-destination
```

Create VLAN 5.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
```

Configure VLAN 5 as the remote probe VLAN of the remote destination group.

```
[DeviceA] mirroring-group 1 remote-probe vlan 5
```

Configure GigabitEthernet 1/0/3 as the monitor port of the remote destination group.

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

Configure GigabitEthernet 1/0/3 as an access port, and assign the port to the remote probe VLAN.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 5
```

Disable the spanning tree feature on GigabitEthernet 1/0/3.

```
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring Device B (the intermediate device)

Create VLANs 2 and 3.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 3
```

Create VLAN 5.

```
[DeviceB] vlan 5
[DeviceB-vlan5] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port, and assign the port to VLANs 2, 3, and 5.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 3 5
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLANs 2, 3, and 5.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 3 5
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C (the source device)

Create VLANs 2 and 3.

```
<DeviceC> system-view
[DeviceC] vlan 2 to 3
```

Assign GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port access vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

Assign GigabitEthernet 1/0/2 to VLAN 3.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port access vlan 3
[DeviceC-GigabitEthernet1/0/2] quit
```

Create a remote source group.

```
[DeviceC] mirroring-group 1 remote-source
```

Create VLAN 5.

```
[DeviceC] vlan 5
[DeviceC-vlan5] quit
```

Configure VLAN 5 as the remote probe VLAN for the remote source group.

```
[DeviceC] mirroring-group 1 remote-probe vlan 5
```

Configure GigabitEthernet 1/0/1 as the source port of the remote source group and the mirroring direction as inbound.

```
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

Configure GigabitEthernet 1/0/3 as the egress port of the remote source group.

```
[DeviceC] mirroring-group 1 monitor-egress gigabitethernet 1/0/3
```

Configure GigabitEthernet 1/0/3 as a trunk port, and assign the port to VLANs 2, 3, and 5.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 3 5
[DeviceC-GigabitEthernet1/0/3] quit
```

Disable the spanning tree feature and MAC address learning on the egress port GigabitEthernet 1/0/3.

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] undo mac-address mac-learning enable
```

```
[DeviceC-GigabitEthernet1/0/3] quit
```

Configuring Device D (the source device)

Create VLAN 2.

```
<DeviceD> system-view
[DeviceD] vlan 2
[DeviceD-vlan2] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port access vlan 2
[DeviceD-GigabitEthernet1/0/1] quit
```

Create remote source group 1.

```
[DeviceD] mirroring-group 1 remote-source
```

Create VLAN 5.

```
[DeviceD] vlan 5
[DeviceD-vlan5] quit
```

Configure VLAN 5 as the remote probe VLAN for the remote source group.

```
[DeviceD] mirroring-group 1 remote-probe vlan 5
```

Configure GigabitEthernet 1/0/1 as the source port of the remote source group and the mirroring direction as inbound.

```
[DeviceD] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

Configure GigabitEthernet 1/0/2 as the egress port of the remote source group.

```
[DeviceD] mirroring-group 1 monitor-egress gigabitethernet 1/0/2
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign the port to VLANs 2 and 5.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 2 5
```

Disable the spanning tree feature and MAC address learning on the egress port GigabitEthernet 1/0/2.

```
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] undo mac-address mac-learning enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify mirroring group configurations on devices:

Display information about mirroring group 1 on Device C.

```
[DeviceC] display mirroring-group 1
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor egress port: GigabitEthernet1/0/3
        Remote probe VLAN: 5
```

Display information about mirroring group 1 on Device A.

```
[DeviceA] display mirroring-group 1
```

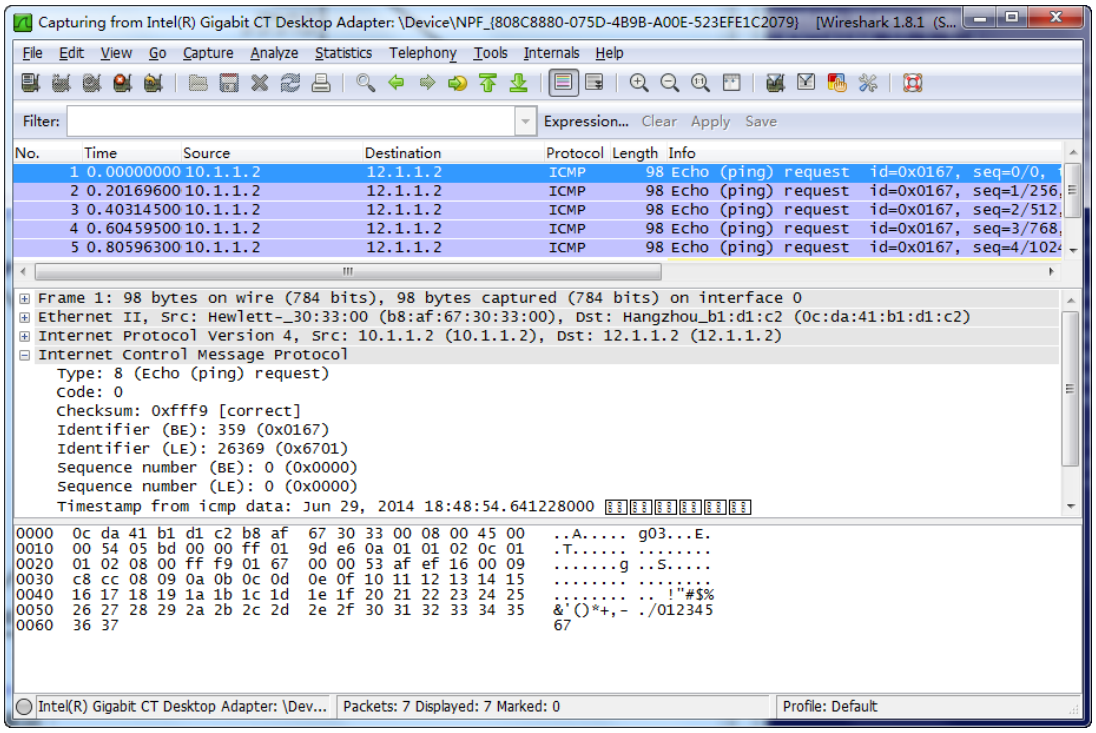
```
Mirroring group 1:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/3
    Remote probe VLAN: 5
```

2. Use Wireshark for packet analysis:

Ping a Marketing department host (12.1.1.2) from a Technical department host (10.1.1.2). (Details not shown.)

Use Wireshark on the data monitoring device to capture the ping packets.

Figure 4 Ping packet analysis in Wireshark



The analysis shows that the data monitoring device can monitor the outgoing traffic from the Technical department.

Configuration files

IMPORTANT:

The **`port link-mode`** command is not supported on the following switches:

- S5130S-HI switch series.
- S5130S-EI switch series.
- S5135S-EI switch series.
- S3100V3-EI switch series.
- E128C switch.
- E152C switch.
- E500C switch series.
- E500D switch series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M switch series.
- IE4320 switch series.

- Device A:

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 5
#
vlan 2 to 3
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 12.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 5
 undo stp enable
```

```
 mirroring-group 1 monitor-port
#
```

- Device B:

```
#
vlan 2 to 3
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
#
```

- Device C:

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 5
#
vlan 2 to 3
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
 mirroring-group 1 monitor-egress
```

- Device D:

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 5
#
vlan 2
#
```

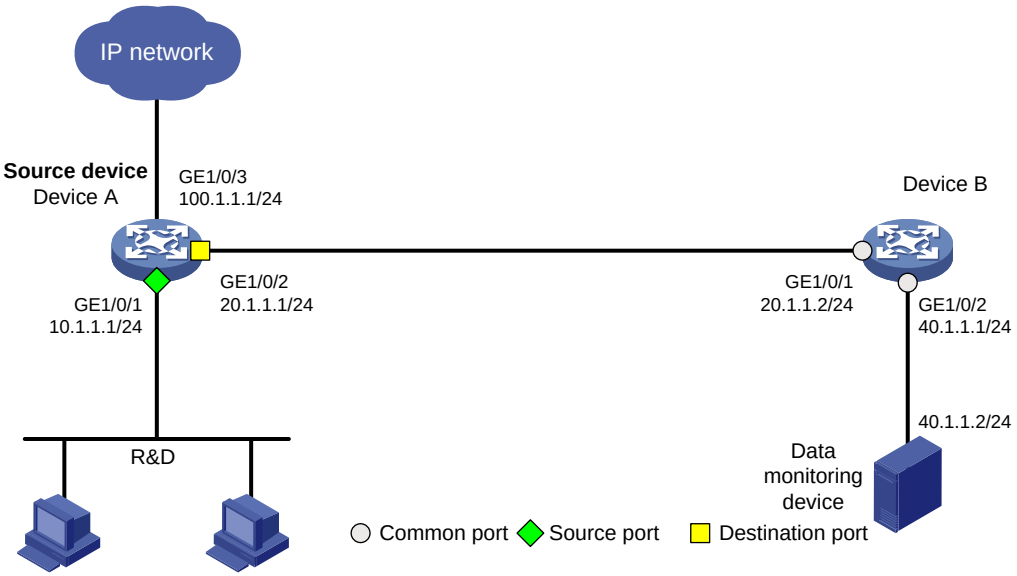
```
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
 mirroring-group 1 monitor-egress
#
```

Example: Configuring Layer 3 remote port mirroring (ERSPAN)

Network configuration

As shown in Figure 5, configure Layer 3 remote port mirroring, so that the data monitoring device can monitor the traffic from the R&D department to Internet.

Figure 5 Network diagram



Analysis

When configuring Layer 3 remote port mirroring, first create a mirroring group, and then configure the source ports and monitor port for the mirroring group. Configure encapsulation parameters of mirrored packets when configuring the monitor port of the mirroring group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Procedures

Configuring Device A

Assign IP address 20.1.1.1 to interface GigabitEthernet 1/0/2.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 20.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

Assign IP addresses to other interfaces in the same way. (Details not shown.)

Configure OSPF.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Create local mirroring group 1.

```
[DeviceA] mirroring-group 1 local
```

Configure a source port for local mirroring group 1.

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

Configure the monitor port and encapsulation parameters of mirrored packets for local mirroring group 1.

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2 destination-ip 40.1.1.2
source-ip 20.1.1.1
```

Configuring Device B

Configure OSPF.

```
<DeviceB> system-view
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Verifying the configuration

Display information about mirroring group 1 on Device A.

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
                  Encapsulation: Destination IP address 40.1.1.2
```

```
Source IP address 20.1.1.1
Destination MAC address 1025-4125-412b
```

Configuration files

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.1.1.1 255.255.255.0
 mirroring-group 1 monitor-port  destination-ip 40.1.1.2 source-ip 20.1.1.1
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 100.1.1.1 255.255.255.0
#
mirroring-group 1 local
mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 40.1.1.1 255.255.255.0
#
```

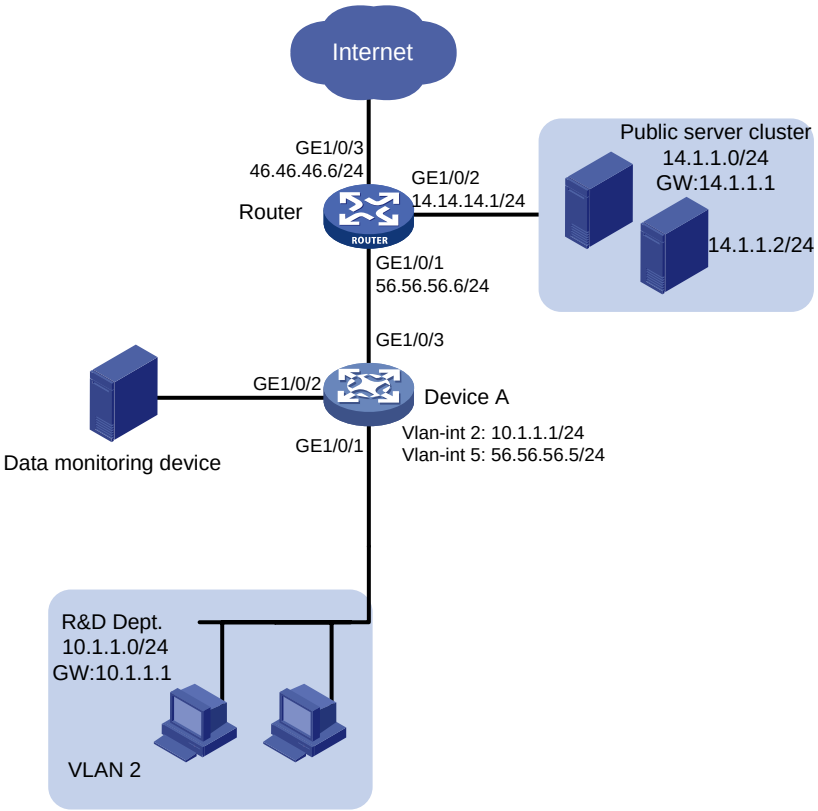
Example: Configuring local flow mirroring

Network configuration

As shown in Figure 6, configure local flow mirroring to mirror the following traffic:

- HTTP traffic from the Technical department.
- Packets that the Technical department hosts receive from the public server cluster during non-working hours from 18:00 to 08:30 (the next day) on working days.

Figure 6 Network diagram



Analysis

To configure local flow mirroring, you must perform the following tasks on Device A:

- Define traffic classes and configure match criteria to classify packets to be mirrored.
- Configure traffic behaviors to mirror the matching packets to the port that connects to the data monitoring device.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

1. Make sure Device A, Router, and the public server cluster can reach each other at Layer 3 and Device A and Internet can reach each other at Layer 3. (Details not shown.)

2. Assign interfaces to VLANs and assign IP addresses to VLAN interfaces:

Create VLAN 2 and VLAN 5.

```
<DeviceA> system-view
[DeviceA] vlan 2 5
```

Create VLAN-interface 2, and assign an IP address to it, which will act as the gateway of VLAN 2.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
```

Create VLAN-interface 5, and assign IP address 56.56.56.5 to it.

```
[DeviceA] interface vlan-interface 5
[DeviceA-Vlan-interface5] ip address 56.56.56.5 24
[DeviceA-Vlan-interface5] quit
```

Assign GigabitEthernet 1/0/1 to VLAN 2 and GigabitEthernet 1/0/3 to VLAN 5.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 2
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 5
[DeviceA-GigabitEthernet1/0/3] quit
```

3. Configure a QoS policy to mirror HTTP traffic from the Technical department:

Create ACL 3000 and configure a rule to match packets from the Technical department to the Internet.

```
[DeviceA] acl number 3000
[DeviceA-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80 source 10.1.1.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

Create traffic class **classifier_internet**, and configure the match criterion as ACL 3000.

```
[DeviceA] traffic classifier classifier_internet
[DeviceA-classifier-classifier_internet] if-match acl 3000
[DeviceA-classifier-classifier_internet] quit
```

Create traffic behavior **behavior_internet**, and configure the action of mirroring traffic to GigabitEthernet 1/0/2.

```
[DeviceA] traffic behavior behavior_internet
[DeviceA-behavior-behavior_internet] mirror-to interface gigabitethernet 1/0/2
[DeviceA-behavior-behavior_internet] quit
```

Create QoS policy **policy_internet**, and associate traffic class **classifier_internet** with traffic behavior **behavior_internet** in the QoS policy.

```
[DeviceA] qos policy policy_internet
[DeviceA-qospolicy-policy_internet] classifier classifier_internet behavior
behavior_internet
[DeviceA-qospolicy-policy_internet] quit
```

4. Configure a QoS policy to mirror traffic that the Technical department hosts receive from the public server cluster:

Create a periodic time range **off-work1**, setting it to be active between 0:00 and 8:30 during working days.

```
[DeviceA] time-range off-work1 0:00 to 8:30 working-day
```

Create a periodic time range **off-work2**, setting it to be active between 18:00 and 24:00 during working days.

```
[DeviceA] time-range off-work2 18:00 to 24:00 working-day
```

Create ACL 3001, and configure two rules to match packets from the public server cluster to the Technical department hosts in non-working hours on working days.

```
[DeviceA] acl number 3001
[DeviceA-acl-ipv4-adv-3001] rule permit ip destination 10.1.1.0 0.0.0.255 source 14.1.1.0 0.0.0.255 time-range off-work1
[DeviceA-acl-ipv4-adv-3001] rule permit ip destination 10.1.1.0 0.0.0.255 source 14.1.1.0 0.0.0.255 time-range off-work2
[DeviceA-acl-ipv4-adv-3001] quit
```

Create traffic class **classifier_server**, and configure the match criterion as ACL 3001.

```
[DeviceA] traffic classifier classifier_server
[DeviceA-classifier-classifier_server] if-match acl 3001
[DeviceA-classifier-classifier_server] quit
```

Create traffic behavior **behavior_server**, and configure the action of mirroring traffic to GigabitEthernet 1/0/2.

```
[DeviceA] traffic behavior behavior_server
[DeviceA-behavior-behavior_server] mirror-to interface gigabitethernet 1/0/2
[DeviceA-behavior-behavior_server] quit
```

Create QoS policy **policy_server**, and associate traffic class **classifier_server** with traffic behavior **behavior_server** in the QoS policy.

```
[DeviceA] qos policy policy_server
[DeviceA-qospolicy-policy_server] classifier classifier_server behavior behavior_server
[DeviceA-qospolicy-policy_server] quit
```

5. Apply the QoS policies:

Apply QoS policy **policy_internet** to the inbound direction of GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy_internet inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

Apply QoS policy **policy_server** to the inbound direction of GigabitEthernet 1/0/3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] qos apply policy policy_server inbound
[DeviceA-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Display local flow mirroring information on Device A.

```
[DeviceA] display qos policy interface
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: policy_internet
   Classifier: classifier_internet
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: behavior_internet
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/2
```

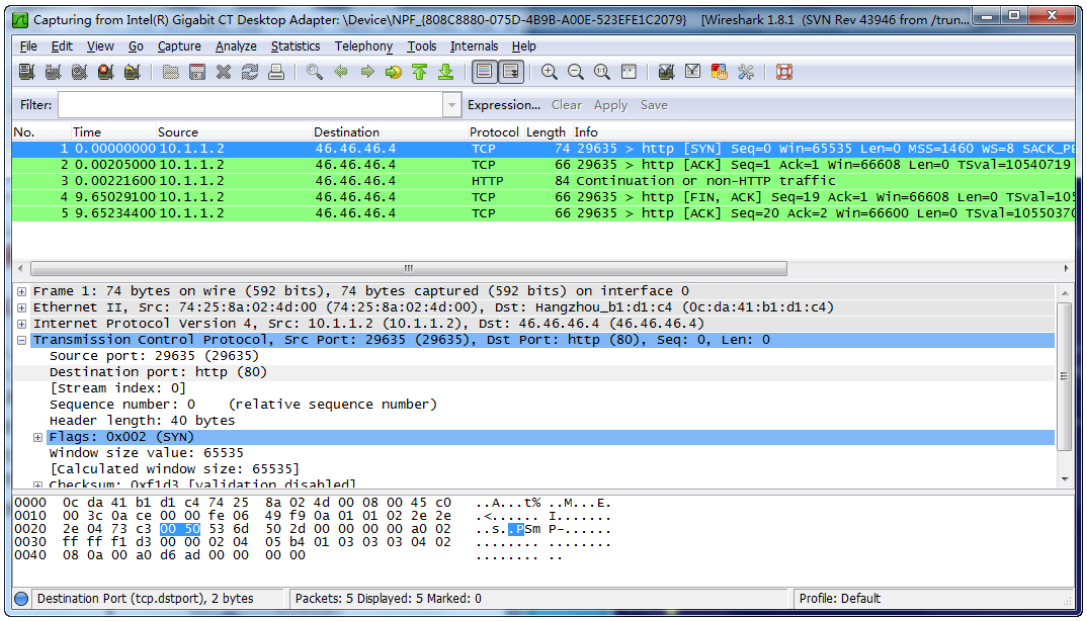
```
Interface: GigabitEthernet1/0/3
Direction: Inbound
Policy: policy_server
 Classifier: classifier_server
   Operator: AND
   Rule(s) :
    If-match acl 3001
   Behavior: behavior_server
    Mirroring:
      Mirror to the interface: GigabitEthernet1/0/2
```

2. Use Wireshark for packet analysis:

Use a Technical department host (10.1.1.2) to access the IP address 46.46.46.4 and port 80 through Telnet. (Details not shown.)

Use Wireshark on the data monitoring device to capture the packets.

Figure 7 HTTP traffic analysis in Wireshark

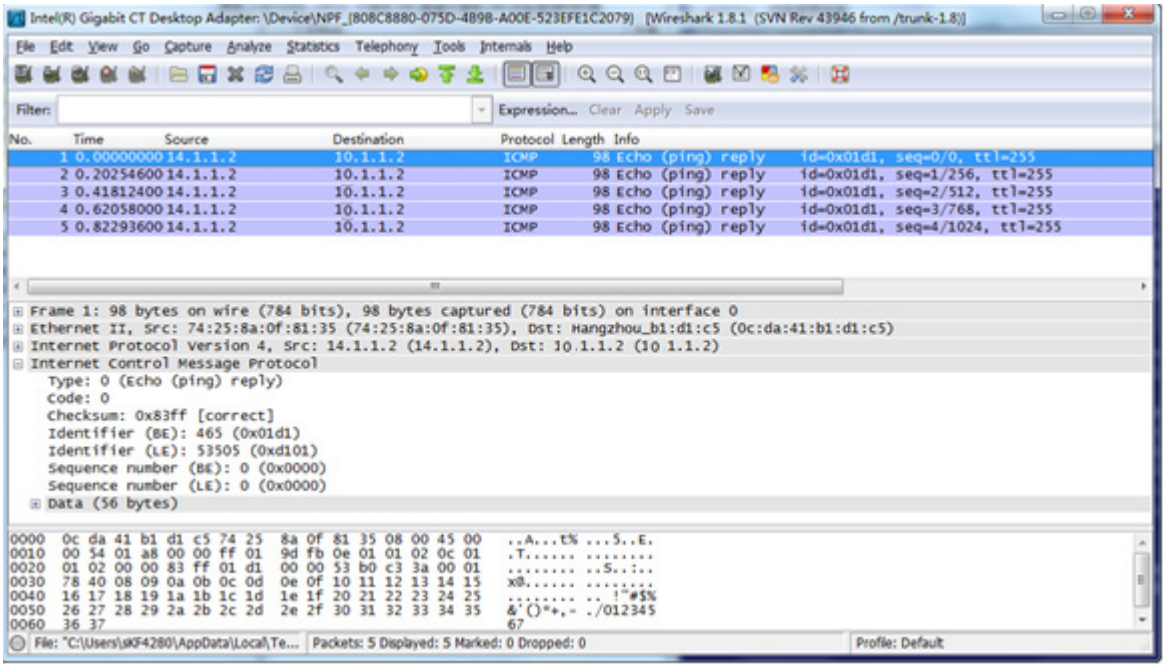


The analysis shows that the data monitoring device can monitor the HTTP traffic from the Technical department.

On a non-working hour of a working day, ping a public server (14.1.1.2) from a Technical department host (10.1.1.2). (Details not shown.)

Use Wireshark on the data monitoring device to capture the ping packets.

Figure 8 Ping packet analysis in Wireshark



The analysis shows that the data monitoring device can monitor the traffic that the public server cluster send to the Technical department during non-working hours on working days.

Configuration files

IMPORTANT:

The **`port link-mode`** command is not supported on the following switches:

- S5130S-HI switch series.
- S5130S-EI switch series.
- S5135S-EI switch series.
- S3100V3-EI switch series.
- E128C switch.
- E152C switch.
- E500C switch series.
- E500D switch series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M switch series.
- IE4320 switch series.

```
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
```

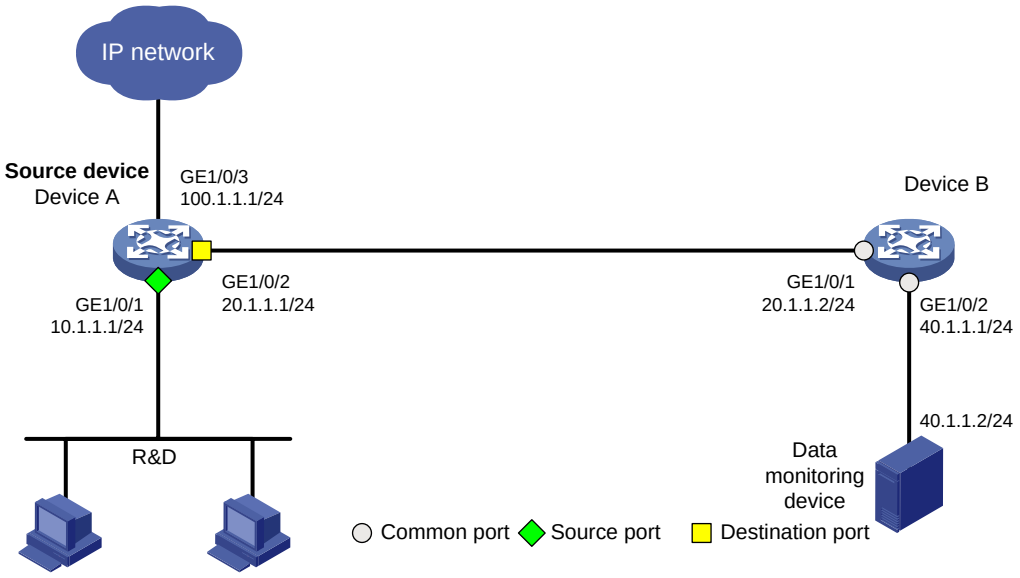
```
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface5
 ip address 56.56.56.5 255.255.255.0
#
 time-range off-work1 00:00 to 08:30 working-day
 time-range off-work2 18:00 to 24:00 working-day
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit ip source 14.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 time-range
off-work1
 rule 5 permit ip source 14.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 time-range
off-work2
#
traffic classifier classifier_internet operator and
 if-match acl 3000
traffic classifier classifier_server operator and
 if-match acl 3001
#
traffic behavior behavior_internet
 mirror-to interface GigabitEthernet1/0/2
traffic behavior behavior_server
 mirror-to interface GigabitEthernet1/0/2
#
qos policy policy_internet
 classifier classifier_internet behavior behavior_internet
qos policy policy_server
 classifier classifier_server behavior behavior_server
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 qos apply policy policy_internet inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 5
 qos apply policy policy_server inbound
#
```

Example: Configuring Layer 3 remote flow mirroring (common Layer 3 routes)

Network configuration

As shown in Figure 9, configure Layer 3 remote flow mirroring to enable the server to monitor the R&D Department's HTTP traffic to network 100.1.1.1.

Figure 9 Network diagram



Analysis

To configure remote flow mirroring, you must perform the following tasks:

- Define traffic classes and configure match criteria to classify packets to be mirrored.
- Configure traffic behaviors to mirror the matching packets to a port and re-encapsulate the matching packets so that the packets can be forwarded to the data monitoring server.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

Hardware	Software version
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series	Not supported

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring Device A

1. Assign IP addresses to interfaces.

   The following example assigns IP address 20.1.1.1 to GigabitEthernet 1/0/2.

   ```
   <DeviceA> system-view
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] port link-mode route
   [DeviceA-GigabitEthernet1/0/2] ip address 20.1.1.1 24
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

2. Configure the QoS policy **policy_research**:

   # Create ACL 3000, and configure a rule to match packets from the R&D department to access the Internet.

   ```
   [DeviceA] acl number 3000
   ```

```
[DeviceA-acl-adv-3000] rule permit tcp destination 100.1.1.0 0.0.0.255
destination-port eq 80 source 10.1.1.0 0.0.0.255
[DeviceA-acl-adv-3000] quit
```

Create the traffic class **classifier_research**, and configure the match criterion as ACL 3000.

```
[DeviceA] traffic classifier classifier_research
[DeviceA-classifier-classifier_research] if-match acl 3000
[DeviceA-classifier-classifier_research] quit
```

Create the traffic behavior **behavior_research**, configure the action of mirroring traffic to GigabitEthernet 1/0/2 and encapsulate the packets with source IP address 20.1.1.1 and destination IP address 40.1.1.2.

```
[DeviceA] traffic behavior behavior_research
[DeviceA-behavior-behavior_research] mirror-to interface gigabitethernet 1/0/2
destination-ip 40.1.1.2 source-ip 20.1.1.1
[DeviceA-behavior-behavior_research] quit
```

Create the QoS policy **policy_research**.

```
[DeviceA] qos policy policy_research
```

Associate the traffic class **classifier_research** with the traffic behavior **behavior_research** in the QoS policy.

```
[DeviceA-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[DeviceA-qospolicy-policy_research] quit
```

Apply the QoS policy to the inbound direction of GigabitEthernet 1/0/1.

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Assign IP addresses to interfaces. The following example assigns IP address 20.1.1.2 to GigabitEthernet 1/0/1.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-mode route
[DeviceB-GigabitEthernet1/0/1] ip address 20.1.1.2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure the OSPF protocol.

```
<DeviceB> system-view
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Verifying the configuration

Display remote flow mirroring configuration on Device A.

```
[DeviceA] display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
```

```
Policy: policy_research
 Classifier: classifier_research
   Operator: AND
   Rule(s) :
    If-match acl 3000
   Behavior: behavior_research
    Mirroring:
      Mirror to the interface: GigabitEthernet1/0/2
                Encapsulation: Destination IP address 40.1.1.2
                               Source IP address 20.1.1.1
                               Destination-MAC 1025-4125-412b
```

Configuration files

- Device A:

```
#
traffic classifier classifier_research operator and
 if-match acl 3000
#
traffic behavior behavior_research
 mirror-to interface GigabitEthernet1/0/2 destination-ip 40.1.1.2 source-ip 20.1.1.1
#
qos policy policy_research
 classifier classifier_research behavior behavior_research
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 qos apply policy policy_research inbound
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 20.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 40.1.1.1 255.255.255.0
#
```

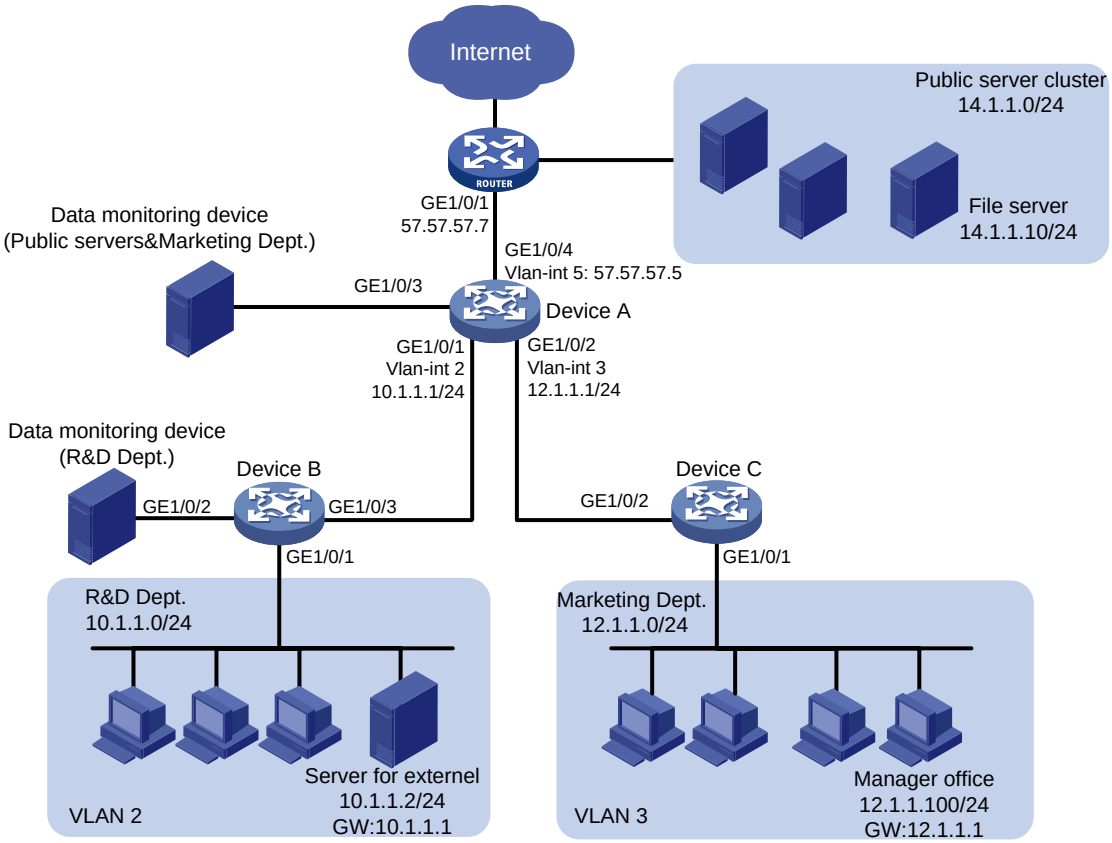
Example: Configuring flow mirroring in a flexible way

Network configuration

As shown in Figure 10, configure flow mirroring to monitor the network traffic by using the data monitoring devices as follows:

- On the data monitoring device connected to Device A:
  - Monitor the traffic from public servers.
  - Monitor the traffic from the file server only in the non-working hours (18:00 to 8:30 of the next day) on working days.
  - Monitor the traffic from the Marketing department to the Internet, except the traffic from the Marketing department manager office to the Internet.
- On the data monitoring device connected to Device B:
  - Monitor the traffic from the Technical department hosts and the server for external access.
  - Monitor the outgoing traffic from the server in non-working hours (18:00 to 8:30 of the next day) on working days.

Figure 10 Network diagram



Analysis

To filter data from a specific source, use one of the following methods:

- Apply a QoS policy of denying traffic to the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.
- Configure a class-behavior association to permit the data from the specified source, and then issue the class-behavior association before the class-behavior association for mirroring. Data from the specified source is not mirrored.
- Use the **`packet-filter`** command on the outgoing interface of the mirrored data. The data from the specified source is not received by the data monitoring device.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI,	Release 63xx

Hardware	Software version
and S5120V3-54P-PWR-SI)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx

Procedures

Configuring Device A to mirror traffic from the public servers

1. Configure a QoS policy to mirror traffic from all public servers:

   # Create ACL 2000 to match packets from subnet 14.1.1.0/24.

   ```
   <DeviceA> system-view
   [DeviceA] acl number 2000
   [DeviceA-acl-ipv4-basic-2000] rule permit source 14.1.1.0 0.0.0.255
   [DeviceA-acl-ipv4-basic-2000] quit
   ```

   # Create traffic class **classifier_servers**, and configure the match criterion as ACL 2000.

   ```
   [DeviceA] traffic classifier classifier_servers
   ```

```
[DeviceA-classifier-classifier_servers] if-match acl 2000
[DeviceA-classifier-classifier_servers] quit
```

Create traffic behavior **behavior_servers**, and configure the action of mirroring traffic to GigabitEthernet 1/0/3.

```
[DeviceA] traffic behavior behavior_servers
[DeviceA-behavior-behavior_servers] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-behavior_servers] quit
```

Create QoS policy **policy_servers**, and associate traffic class **classifier_servers** with traffic behavior **behavior_servers** in the QoS policy.

```
[DeviceA] qos policy policy_servers
[DeviceA-qospolicy-policy_servers] classifier classifier_servers behavior
behavior_servers
[DeviceA-qospolicy-policy_servers] quit
```

Apply QoS policy **policy_servers** to the inbound direction of GigabitEthernet 1/0/4.

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] qos apply policy policy_servers inbound
[DeviceA-GigabitEthernet1/0/4] quit
```

2. Configure a QoS policy to filter packets from the file server in working hours:

Create a periodic time range **work-time**, setting it to be active between 8:30 and 18:00 during working days.

```
[DeviceA] time-range work-time 8:30 to 18:00 working-day
```

Create ACL 2001, and configure a rule to match packets from 14.1.1.10 in working hours on working days.

```
[DeviceA] acl number 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 14.1.1.10 0.0.0.0 time-range
work-time
[DeviceA-acl-ipv4-basic-2001] quit
```

Create traffic class **classifier_fileserver**, and configure the match criterion as ACL 2001.

```
[DeviceA] traffic classifier classifier_fileserver
[DeviceA-classifier-classifier_fileserver] if-match acl 2001
[DeviceA-classifier-classifier_fileserver] quit
```

Create traffic behavior **behavior_fileserver**, and configure the action of denying traffic.

```
[DeviceA] traffic behavior behavior_fileserver
[DeviceA-behavior-behavior_fileserver] filter deny
[DeviceA-behavior-behavior_fileserver] quit
```

Create QoS policy **policy_fileserver**, and associate traffic class **classifier_fileserver** with traffic behavior **behavior_fileserver** in the QoS policy.

```
[DeviceA] qos policy policy_fileserver
[DeviceA-qospolicy-policy_fileserver] classifier classifier_fileserver behavior
behavior_fileserver
[DeviceA-qospolicy-policy_fileserver] quit
```

Apply QoS policy **policy_fileserver** to the outbound direction of GigabitEthernet 1/0/3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] qos apply policy policy_fileserver outbound
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring Device A to mirror the Internet traffic from the Marketing department

1. Create a traffic class and a traffic behavior for the packets:

Create ACL 3000, and configure a rule to match packets from subnet 12.1.1.0/24.

```
[DeviceA] acl number 3000
[DeviceA-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80 source 12.1.1.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

Create traffic class **classifier_market**, and configure the match criterion as ACL 3000.

```
[DeviceA] traffic classifier classifier_market
[DeviceA-classifier-classifier_market] if-match acl 3000
[DeviceA-classifier-classifier_market] quit
```

Create traffic behavior **behavior_market**, and configure the action of mirroring traffic to GigabitEthernet 1/0/3.

```
[DeviceA] traffic behavior behavior_market
[DeviceA-behavior-behavior_market] mirror-to interface gigabitethernet 1/0/3
[DeviceA-behavior-behavior_market] quit
```

2. Create a traffic class and a traffic behavior for the packets from the manager office:

Create ACL 3001, and configure a rule to match packets from 12.1.1.100.

```
[DeviceA] acl number 3001
[DeviceA-acl-ipv4-adv-3001] rule permit tcp destination-port eq 80 source 12.1.1.100
0.0.0.0
[DeviceA-acl-ipv4-adv-3001] quit
```

Create traffic class **classifier_market_mgr**, and configure the match criterion as ACL 3001.

```
[DeviceA] traffic classifier classifier_market_mgr
[DeviceA-classifier-classifier_market_mgr] if-match acl 3001
[DeviceA-classifier-classifier_market_mgr] quit
```

Create traffic behavior **behavior_market_mgr**, and configure the action of permitting traffic to pass through.

```
[DeviceA] traffic behavior behavior_market_mgr
[DeviceA-behavior-behavior_market_mgr] filter permit
[DeviceA-behavior-behavior_market_mgr] quit
```

3. Create a QoS policy and associate the traffic classes and traffic behaviors:

Create QoS policy **policy_market**.

```
[DeviceA] qos policy policy_market
```

Associate traffic class **classifier_market_mgr** with traffic behavior **behavior_market_mgr** in the QoS policy.

```
[DeviceA-qospolicy-policy_market] classifier classifier_market_mgr behavior
behavior_market_mgr
```

Associate traffic class **classifier_market** with traffic behavior **behavior_market** in the QoS policy.

```
[DeviceA-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
```

Display the sequence of issuing the class–behavior associations.

```
[DeviceA-qospolicy-policy_market] display this
#
qos policy policy_market
 classifier classifier_market_mgr behavior behavior_market_mgr
 classifier classifier_market behavior behavior_market
#
return
[DeviceA-qospolicy-policy_market] quit
```

The output shows that the class–behavior association for the manager office are issued first. The packets from the manager office to access the Internet are not mirrored.

4. Apply QoS policy **policy_market** to the inbound direction of GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] qos apply policy policy_market inbound
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B to mirror traffic from the Technical department

1. Configure local mirroring on Device B:

   # Create local mirroring group 1.

```
<DeviceB> system-view
[DeviceB] mirroring-group 1 local
```

   # Configure the mirroring group to monitor the incoming traffic of the port GigabitEthernet 1/0/1.

```
[DeviceB] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

   # Configure GigabitEthernet 1/0/2 as the monitor port of the mirroring group.

```
[DeviceB] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

2. Configure an ACL to filter the outgoing traffic from the server (10.1.1.2) in working hours:

   # Create a periodic time range **work-time**, setting it to be active between 8:30 and 18:00 during working days.

```
[DeviceB] time-range work-time 8:30 to 18:00 working-day
```

   # Create ACL 2000, and configure a rule to deny packets from 10.1.1.2 in working hours on working days.

```
[DeviceB] acl number 2000
[DeviceB-acl-ipv4-basic-2000] rule deny source 10.1.1.2 0.0.0.0 time-range work-time
[DeviceB-acl-ipv4-basic-2000] quit
```

   # Apply ACL 2000 to filter the outgoing traffic on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet1/0/2
[DeviceB-GigabitEthernet1/0/2] packet-filter 2000 outbound
[DeviceB-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify flow mirroring configurations on devices:

   # Display flow mirroring information on Device A.

```
[DeviceA] display qos policy interface
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: policy_market
   Classifier: classifier_market_mgr
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: behavior_market_mgr
      Filter enable: Permit
   Classifier: classifier_market
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: behavior_market
      Mirroring:
```

```
        Mirror to the interface: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/3
  Direction: Outbound
  Policy: policy_fileserver
   Classifier: classifier_fileserver
     Operator: AND
     Rule(s) : If-match acl 2001
     Behavior: behavior_fileserver
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/3

Interface: GigabitEthernet1/0/4
  Direction: Inbound
  Policy: policy_servers
   Classifier: classifier_servers
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: behavior_servers
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/3
```

Display information about mirroring group 1 on Device B.

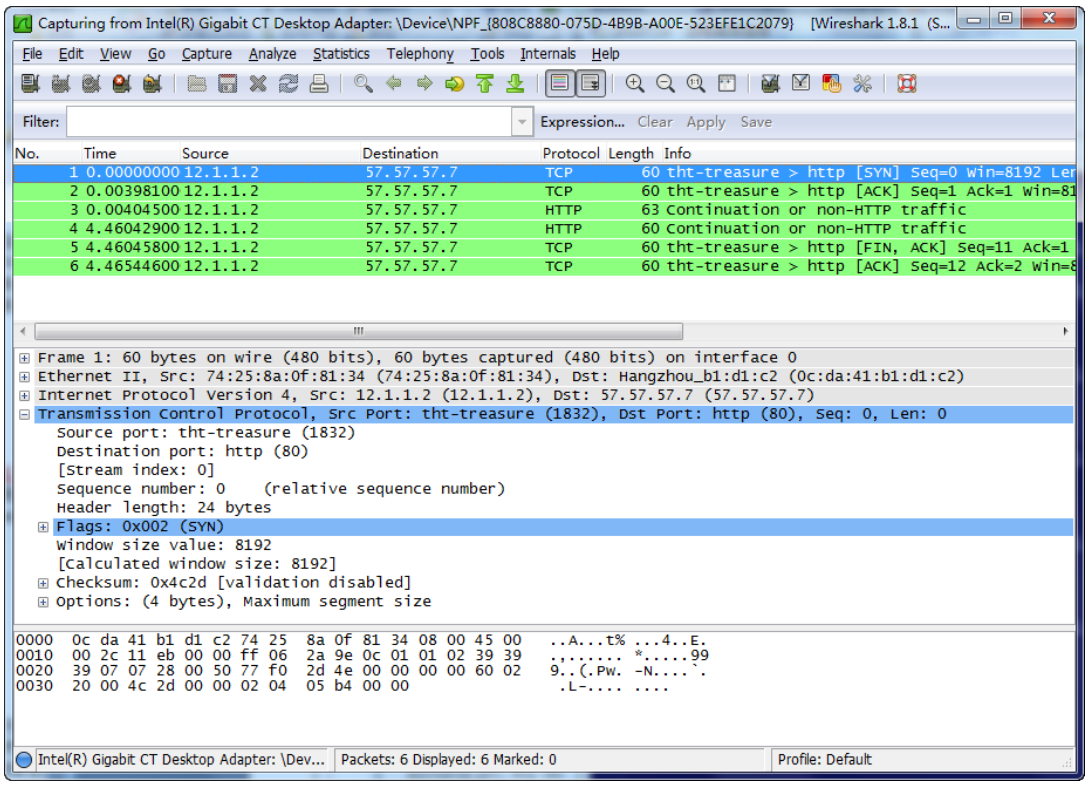
```
[DeviceB] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
```

2. Use Wireshark for packet analysis:

Use a Marketing department host (12.1.1.2) and the manager's host (12.1.1.100) to access the IP address 57.57.57.7 and port 80 through Telnet. (Details not shown.)

Use Wireshark on the data monitoring device connected to Device A to capture the packets.

Figure 11 HTTP traffic analysis in Wireshark



The analysis shows that the data monitoring device monitors the traffic only from the Marketing department host (12.1.1.2). The traffic from the manager office is not monitored.

Configuration files

IMPORTANT:

The **`port link-mode`** command is not supported on the following switches:

- S5130S-HI switch series.
- S5130S-EI switch series.
- S5135S-EI switch series.
- S3100V3-EI switch series.
- E128C switch.
- E152C switch.
- E500C switch series.
- E500D switch series.
- IE4300-12P-AC switch
- IE4300-12P-PWR switch.
- IE4300-M switch series.
- IE4320 switch series.

- Device A:

```
#
 time-range work-time 08:30 to 18:00 working-day
```

```
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
acl number 2001
 rule 0 permit source 14.1.1.10 0 time-range work-time
#
acl number 3000
 rule 0 permit tcp source 12.1.1.0 0.0.0.255 destination-port eq www
acl number 3001
 rule 0 permit tcp source 12.1.1.100 0 destination-port eq www
#
traffic classifier classifier_servers operator and
 if-match acl 2000
traffic classifier classifier_fileserver operator and
 if-match acl 2001
traffic classifier classifier_market operator and
 if-match acl 3000
traffic classifier classifier_market_mgr operator and
 if-match acl 3001
#
traffic behavior behavior_servers
 mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_fileserver
 filter deny
traffic behavior behavior_market
 mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_market_mgr
 filter permit
#
qos policy policy_fileserver
 classifier classifier_fileserver behavior behavior_fileserver
qos policy policy_market
 classifier classifier_market_mgr behavior behavior_market_mgr
 classifier classifier_market behavior behavior_market
qos policy policy_servers
 classifier classifier_servers behavior behavior_servers
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 qos apply policy policy_market inbound
#
```

```
interface GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy_fileserver outbound
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 5
 ip address 57.57.57.5 255.255.255.0
 qos apply policy policy_servers inbound
#
```

- Device B:

```
#
 mirroring-group 1 local
#
 time-range work-time 08:30 to 18:00 working-day
#
acl number 2000
 rule 0 deny source 10.1.1.2 0 time-range work-time
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 packet-filter 2000 outbound
 mirroring-group 1 monitor-port
#
```

Contents

Introduction

This document provides sFlow configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of sFlow.

Restrictions and guidelines

When you configure sFlow, follow these restrictions and guidelines:

- You can specify only the random sampling mode (the default).
- For the remote sFlow collector to receive sFlow packets, the IP address of the sFlow collector specified on the sFlow agent must be the same with that of the remote sFlow collector.
- If the number of packets sampled by an interface is too much in a heavy traffic network, increase the flow sampling interval. If an interface samples insufficient packets in a light traffic network, decrease the flow sampling interval.
- If an interface collects data too frequently in a heavy traffic network, increase the counter sampling interval. If the sampling statistics is not accurate in a light traffic network, decrease the counter sampling interval.

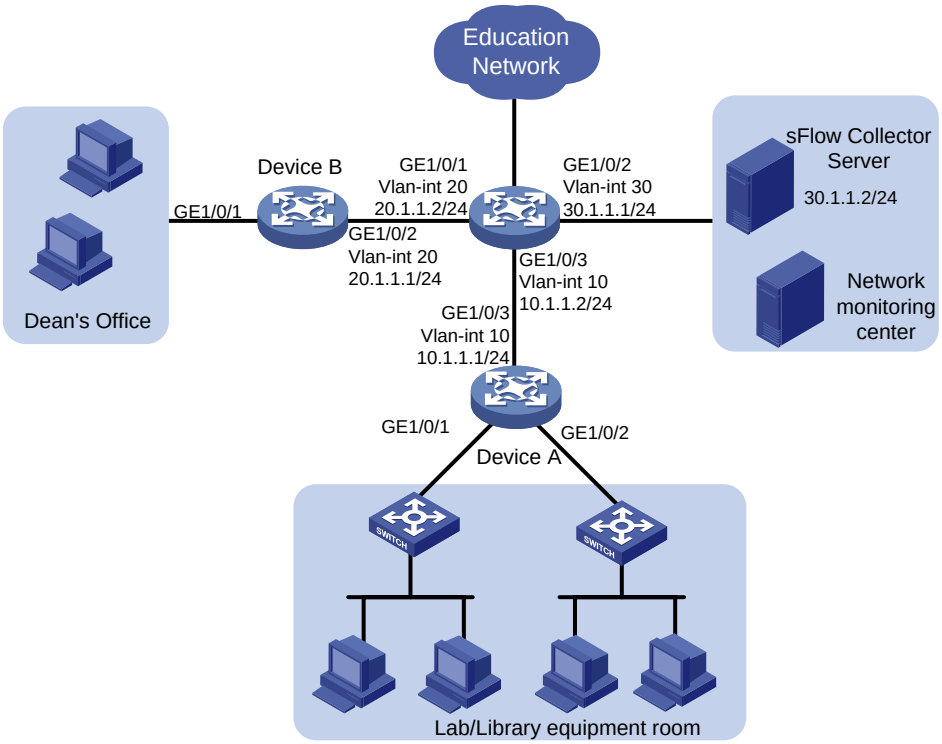
Example: Configuring sFlow

Network configuration

As shown in Figure 1, perform the following tasks:

- Configure flow sampling to sample packets on Device A and Device B.
- Configure counter sampling to periodically collect the counter information on Device A and Device B.

Figure 1 Network diagram



Analysis

To obtain interface counter information and packet information, you must configure both flow sampling and counter sampling.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-54C switch	
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx

Hardware	Software version
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Device A

Create VLAN 10. Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-vlan10] quit
```

Assign an IP address to VLAN-interface 10.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
[DeviceA-Vlan-interface10] quit
```

Assign IP addresses to other interfaces. (Details not shown.)

Assign an IP address to the sFlow agent.

```
[DeviceA] sflow agent ip 10.1.1.1
```

Specify the sFlow collector ID as 1, IP address as 30.1.1.2, and port number as 5000.

```
[DeviceA] sflow collector 1 ip 30.1.1.2 port 5000
```

Enable counter sampling and set the counter sampling interval to 120 seconds on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] sflow counter interval 120
```

Specify sFlow collector 1 for counter sampling on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] sflow counter collector 1
[DeviceA-GigabitEthernet1/0/1] quit
```

Enable counter sampling and set the counter sampling interval to 120 seconds on GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] sflow counter interval 120
```

Specify sFlow collector 1 for counter sampling on GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] sflow counter collector 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Enable flow sampling and set the sampling interval to 10000 on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] sflow sampling-rate 10000
```

Specify sFlow collector 1 for flow sampling on GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] sflow flow collector 1
[DeviceA-GigabitEthernet1/0/1] quit
```

Enable flow sampling and set the sampling interval to 10000 on GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] sflow sampling-rate 10000
```

Specify sFlow collector 1 for flow sampling on GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] sflow flow collector 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B

Create VLAN 20. Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to VLAN 20.

```
<DeviceB> system-view
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

Assign an IP address to VLAN-interface 20.

```
[DeviceB] interface vlan-interface 20
[DeviceB-Vlan-interface20] ip address 20.1.1.1 255.255.255.0
[DeviceB-Vlan-interface20] quit
```

Assign an IP address to the sFlow agent.

```
[DeviceB] sflow agent ip 20.1.1.1
```

Specify the sFlow collector ID as 1, IP address as 30.1.1.2, and port number as 5000.

```
[DeviceB] sflow collector 1 ip 30.1.1.2 port 5000
```

Enable counter sampling and set the counter sampling interval to 30 seconds on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] sflow counter interval 30
```

Specify sFlow collector 1 for counter sampling on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] sflow counter collector 1
```

Enable flow sampling and set the sampling interval to 20000 on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] sflow sampling-rate 20000
```

Specify sFlow collector 1 for flow sampling on GigabitEthernet 1/0/1.

```
[DeviceB-GigabitEthernet1/0/1] sflow flow collector 1
[DeviceB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify the following items on Device A:

- GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 enabled with sFlow are active.
- The counter sampling interval is 120 seconds.
- The flow sampling interval is 10000.

```
[DeviceA] display sflow
sFlow datagram version: 5
Global information:
Agent IP: 10.1.1.1(CLI)
Source address:
Collector information:
ID    IP              Port  Aging      Size VPN-instance Description
1     30.1.1.2        5000  N/A        1400              CLI Collector
Port counter sampling information:
Interface   Instance   CID   Interval(s)
GE1/0/1     1          1     120
GE1/0/2     1          1     120
Port flow sampling information:
Interface   Instance   FID   MaxHLen Rate       Mode      Status
GE1/0/1     1          1     128     10000      Random    Active
GE1/0/2     1          1     128     10000      Random    Active
```

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
 sflow agent ip 10.1.1.1
 sflow collector 1 ip 30.1.1.2 port 5000 description "CLI Collector"
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
```

```
 sflow flow collector 1
 sflow sampling-rate 10000
 sflow counter collector 1
 sflow counter interval 120
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 sflow flow collector 1
 sflow sampling-rate 10000
 sflow counter collector 1
 sflow counter interval 120
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
```

- Device B:

```
#
vlan 20
#
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
#
 sflow agent ip 20.1.1.1
 sflow collector 1 ip 30.1.1.2 port 5000 description "CLI Collector"
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
 sflow flow collector 1
 sflow sampling-rate 20000
 sflow counter collector 1
 sflow counter interval 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

Contents

Introduction

This document provides examples for configuring OpenFlow.

OpenFlow separates the control plane and the data forwarding plane. An OpenFlow switch matches packets against one or more flow tables. A flow table contains one or more flow entries that are deployed by the controller and packets are matched based on the matching precedence of flow entries.

These examples use VLAN-interface 1.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of OpenFlow.

General restrictions and guidelines

When you configure OpenFlow, follow these restrictions and guidelines:

- Enable LLDP globally on OpenFlow switches so that the controller can learn the OpenFlow topology through LLDP.
- Configure each OpenFlow switch with an interface for communicating with the controller so that OpenFlow instances can establish connections with the controller.
- Configure the **Loosen** mode when you associate VLAN 4092 and VLAN 4094 with an OpenFlow instance so that the access ports of switches can belong to the OpenFlow instance.

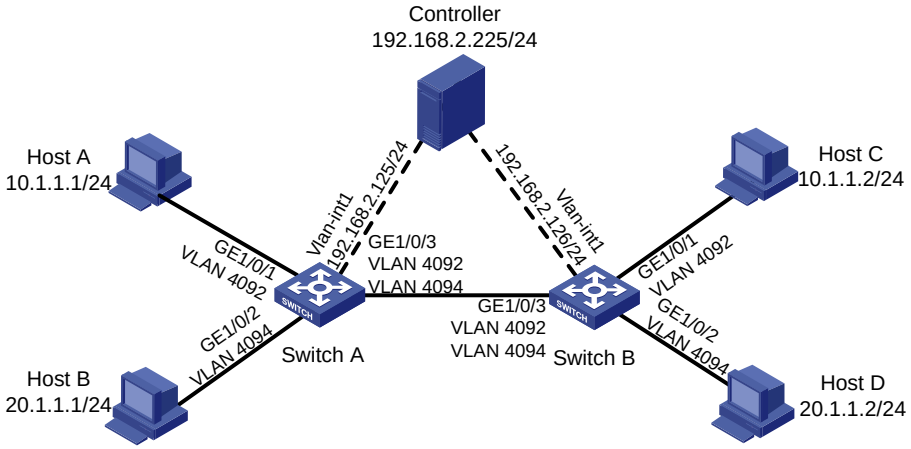
Example: Configuring OpenFlow to deploy flow entries

Network configuration

As shown in Figure 1, configure OpenFlow to meet the following requirements:

- The controller can deploy dynamic flow entries.
- Host A and Host C can communicate with each other based on the flow entries deployed by the controller.
- Host B and Host D can communicate with each other based on the flow entries deployed by the controller.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series	Release 63xx

Hardware	Software version
S5560S-SI switch series	
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series	Release 63xx

Hardware	Software version
WS5810-WiNet switch series	
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Configuring Switch A

Create VLAN 4092 and VLAN 4094.

```
<SwitchA> system-view
[SwitchA] vlan 4092
[SwitchA-vlan4092] quit
[SwitchA] vlan 4094
[SwitchA-vlan4094] quit
```

Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port access vlan 4092
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port access vlan 4094
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4092 4094
[SwitchA-GigabitEthernet1/0/3] quit
```

Enable LLDP globally.

```
[SwitchA] lldp global enable
```

Configure VLAN-interface 1 on Switch A for communicating with the controller.

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.2.125 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Create OpenFlow instance 1. Associate VLAN 4092 and VLAN 4094 with it in loosen mode.

```
[SwitchA] openflow instance 1
[SwitchA-of-inst-1] classification vlan 4092 mask 4093 loosen
```

Specify 192.168.2.225 as the IP address of controller 0 for OpenFlow instance 1 and activate the instance..

```
[SwitchA-of-inst-1] controller 0 address ip 192.168.2.225
[SwitchA-of-inst-1] active instance
```

```
[SwitchA-of-inst-1] quit
```

Configuring Switch B

Create VLAN 4092 and VLAN 4094.

```
<SwitchB> system-view
[SwitchB] vlan 4092
[SwitchB-vlan4092] quit
[SwitchB] vlan 4094
[SwitchB-vlan4094] quit
```

Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port access vlan 4092
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port access vlan 4094
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 4092 4094
[SwitchB-GigabitEthernet1/0/3] quit
```

Enable LLDP globally.

```
[SwitchB] lldp global enable
```

Configure VLAN-interface 1 on Switch B for communicating with the controller.

```
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.2.125 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Create OpenFlow instance 1. Associate VLAN 4092 and VLAN 4094 with it in loosen mode.

```
[SwitchB] openflow instance 1
[SwitchB-of-inst-1] classification vlan 4092 mask 4093 loosen
```

Specify 192.168.2.225 as the IP address of controller 0 for OpenFlow instance 1 and activate the instance.

```
[SwitchB-of-inst-1] controller 0 address ip 192.168.2.225
[SwitchB-of-inst-1] active instance
[SwitchB-of-inst-1] quit
```

Verifying the configuration

Display details for OpenFlow instance 1 on devices, for example, Switch A.

```
[SwitchA] display openflow instance 1
Instance 1 information:

Configuration information:
 Description   : --
 Active status : Active
 Inactive configuration:
  None
```

```
 Active configuration:
  Classification VLAN, loosen mode, total VLANs(2)
   4092, 4094
  In-band management VLAN, total VLANs(0)
   Empty VLAN
  Connect mode: Multiple
  MAC address learning: Enabled
  Flow table:
   Table ID(type): 0(Extensibility), count: 1
  Flow-entry max-limit: 65535
  Datapath ID: 0x000174258a024c00
...
Port information:
 GigabitEthernet1/0/1
 GigabitEthernet1/0/2
 GigabitEthernet1/0/3
Active channel information:
 Controller 0 IP address: 192.168.2.225 port: 6633
```

The output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 belong to OpenFlow instance 1 and can be used to forward packets in the OpenFlow forwarding process.

Display controller information for OpenFlow instance 1 on devices, for example, Switch A.

```
[SwitchA] display openflow instance 1 controller
Instance 1 controller information:
 Reconnect interval: 60 (s)
 Echo interval     : 5  (s)

 Controller ID           : 0
 Controller IP address   : 192.168.2.225
 Controller port         : 6633
 Controller role         : Equal
 Connect type            : TCP
 Connect state           : Established
 Packets sent            : 132
 Packets received        : 434
 SSL policy              : --
 VRF name                : --
```

The output shows that Switch A has established a connection with the controller.

Display flow table information for OpenFlow instance 1 on devices, for example, Switch A.

```
[SwitchA] display openflow instance 1 flow-table
Instance 1 flow table information:

Table 0 information:
 Table type: Extensibility, flow entry count: 1, total flow entry count: 1

MissRule flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem,
 byte count: 0, packet count: 0
```

```
Match information: any
Instruction information:
 Write actions:
  Output interface: Controller, send length: 65509 bytes
```

The output shows that Switch A has only one table-miss flow entry with the priority of 0 and the action of outputting packets to the controller. The action in the table-miss flow entry varies by device model. For more information about the action in the table-miss flow entry, see the related documentation of the controller.

Ping Host C from Host A.

```
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=4.582 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.299 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.389 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=6.688 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=1.294 ms

--- Ping statistics for 10.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.294/3.050/6.688/2.213 ms
```

The output shows that Host A and Host C can reach each other.

Display flow table information for OpenFlow instance 1 again on devices, for example, Switch A.

```
[SwitchA] display openflow instance 1 flow-table
Instance 1 flow table information:

Table 0 information:
 Table type: Extensibility, flow entry count: 4, total flow entry count: 4

MissRule flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem,
 byte count: 0, packet count: 0
Match information: any
Instruction information:
 Write actions:
  Output interface: Controller, send length: 65509 bytes

Flow entry 1 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 1
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c5
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8034
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0806
Instruction information:
 Write actions:
  Output interface: GE1/0/1
```

```
Flow entry 2 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/1
 Ethernet destination MAC address: 7425-8a0f-8034
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 0cda-41b1-d1c5
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/3

Flow entry 3 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c5
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8034
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/1
```

The output shows the following information:

- The ARP request/reply packets and ICMP request/replay packets between Host A and Host C successfully trigger the controller to deploy flow entries.
- Switch A forwards packets based on the flow entries that are deployed by the controller.

Ping Host D from Host B.

```
Ping 20.1.1.2 (20.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 20.1.1.2: icmp_seq=0 ttl=255 time=1.620 ms
56 bytes from 20.1.1.2: icmp_seq=1 ttl=255 time=6.625 ms
56 bytes from 20.1.1.2: icmp_seq=2 ttl=255 time=1.454 ms
56 bytes from 20.1.1.2: icmp_seq=3 ttl=255 time=1.134 ms
56 bytes from 20.1.1.2: icmp_seq=4 ttl=255 time=1.260 ms

--- Ping statistics for 20.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.134/2.419/6.625/2.110 ms
```

The output shows that Host B and Host D can reach each other.

Display flow table information for OpenFlow instance 1 again on devices, for example, Switch A.

```
[SwitchA] display openflow instance 1 flow-table
Instance 1 flow table information:
```

```
Table 0 information:
 Table type: Extensibility, flow entry count: 7, total flow entry count: 7

MissRule flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: flow_send_rem,
 byte count: 0, packet count: 0
Match information: any
Instruction information:
 Write actions:
  Output interface: Controller, send length: 65509 bytes

Flow entry 1 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 1
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c5
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8034
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0806
Instruction information:
 Write actions:
  Output interface: GE1/0/1

Flow entry 2 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/1
 Ethernet destination MAC address: 7425-8a0f-8034
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 0cda-41b1-d1c5
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/3

Flow entry 3 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c5
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8034
```

```
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/1

Flow entry 4 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 1
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c4
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8035
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0806
Instruction information:
 Write actions:
  Output interface: GE1/0/2

Flow entry 5 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/2
 Ethernet destination MAC address: 7425-8a0f-8035
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 0cda-41b1-d1c4
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/3

Flow entry 6 information:
 cookie: 0x2328, priority: 29999, hard time: 0, idle time: 300, flags:
 flow_send_rem, byte count: 1, packet count: 4
Match information:
 Input interface: GE1/0/3
 Ethernet destination MAC address: 0cda-41b1-d1c4
 Ethernet destination MAC address mask: ffff-ffff-ffff
 Ethernet source MAC address: 7425-8a0f-8035
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
Instruction information:
 Write actions:
  Output interface: GE1/0/2
```

The output shows the following information:

- The ARP request/reply packets and ICMP request/replay packets between Host B and Host D successfully trigger the controller to deploy flow entries.
- Switch A forwards packets based on the flow entries that are deployed by the controller.

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Switch A:

```
#
lldp global enable
#
vlan 4092
#
vlan 4094
#
openflow instance 1
 classification vlan 4092 mask 4093 loosen
 controller 0 address ip 192.168.2.225
 active instance
#
interface Vlan-interface1
 ip address 192.168.2.125 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4092
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4092 4094
#
```

- Switch B:

```
#
lldp global enable
#
vlan 4092
#
vlan 4094
#
openflow instance 1
 classification vlan 4092 mask 4093 loosen
```

```
 controller 0 address ip 192.168.2.225
 active instance
#
interface Vlan-interface1
 ip address 192.168.2.126 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4092
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4094
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4092 4094
#
```

Contents

Introduction

This document provides MAC address table configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of the MAC address table.

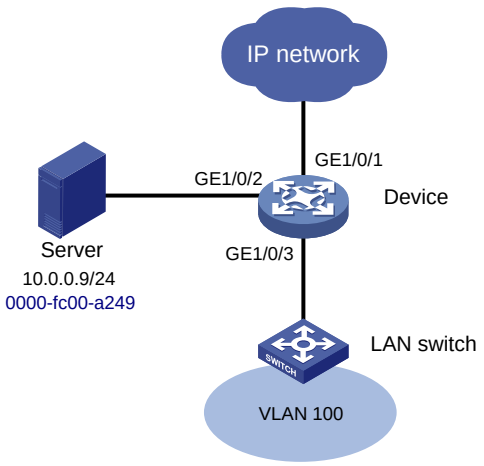
Example: Configuring static MAC address entries

Network configuration

As shown in Figure 1, for secure communication between users in VLAN 100 and the server, perform the following tasks:

- Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 100.
- Add a static MAC address entry on Device to bind the server MAC address to GigabitEthernet 1/0/2.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI switch)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

Create VLAN 100, and assign GigabitEthernet 1/0/2 to VLAN 100.

```
<Device> system-view
```

```
[Device] vlan 100
[Device-vlan100] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port access vlan 100
[Device-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (port connected to the LAN switch) as a trunk port, and assign the port to VLAN 100.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port link-type trunk
[Device-GigabitEthernet1/0/3] port trunk permit vlan 100
[Device-GigabitEthernet1/0/3] quit
```

Add a static entry for MAC address 0000-fc00-a249 on GigabitEthernet 1/0/2 that belongs to VLAN 100.

```
[Device] mac-address static 0000-fc00-a249 interface gigabitethernet 1/0/2 vlan 100
```

Verifying the configuration

Verify that any 10.0.0.0/24 host in VLAN 100 can communicate with the server. (Details not shown.)

Verify that the static MAC address entry has been added.

```
[Device] display mac-address
MAC Address      VLAN ID    State           Port/NickName           Aging
0000-fc00-a249   100        Static          GE1/0/2                 N
7425-8a02-4d00   100        Learned         GE1/0/3                 Y
…
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
sysname Device
#
vlan 1
#
vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 mac-address static 0000-fc00-a249 vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
```

#

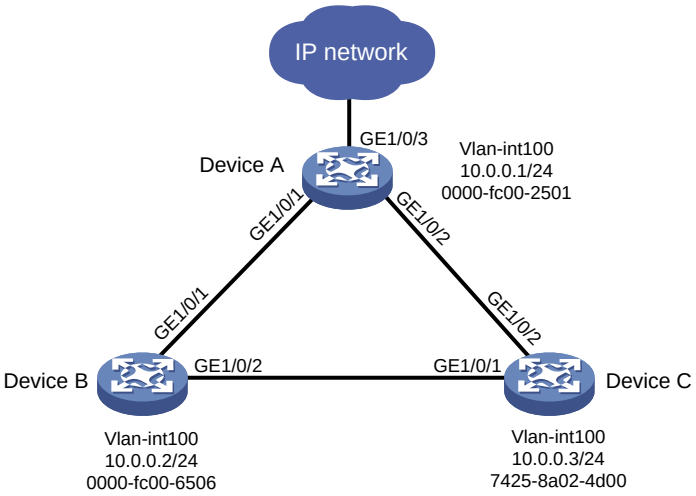
Example: Configuring MAC address move suppression

Network configuration

As shown in Figure 2, Devices A, B, and C form a loop because of cable misconnection, and spanning tree protocols are not enabled on the devices. As a result, MAC addresses are frequently moves among Devices A, B, and C. To deal with loop-triggered MAC flapping, perform the following tasks:

- Display MAC address move records to locate the Layer 2 loop.
- Configure MAC address move suppression on Device A to eliminate the Layer 2 loop.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- For Devices A, B, and C to communicate with each other, assign all inter-connected ports to VLAN 100.
- Configure MAC address move suppression on one or more ports of Device A.
- To monitor the port status change of Device A, enable the log monitoring of the current terminal feature.
- For loop detection, create VLAN-interface 100 and assign an IP address to the interface on each device.
- To display MAC address move records, ping Device B from Device A.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 8106Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 8106Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

Configuring Device A

Enable the monitoring of logs on the current terminal.

```
<DeviceA> terminal monitor
<DeviceA> terminal debugging
```

Create VLAN 100.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign the ports to VLAN 100.

```
[DeviceA] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceA-if-range] port link-type trunk
[DeviceA-if-range] port trunk permit vlan 100
[DeviceA-if-range] quit
```

Set the suppression interval to 300 seconds. A suppressed port will automatically come up after 300 seconds.

```
[DeviceA] mac-address notification mac-move suppression interval 300
```

Set the suppression threshold to 0. A port will be shut down when the system detects a MAC address move on the port within a MAC move detection interval (1 minute by default).

```
[DeviceA] mac-address notification mac-move suppression threshold 0
```

Enable MAC address move suppression on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] mac-address notification mac-move suppression
[DeviceA-GigabitEthernet1/0/1] quit
```

Create VLAN-interface 100, and assign an IP address to the interface.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ip address 10.0.0.1 24
[DeviceA-Vlan-interface100] quit
```

Configuring Device B and Device C

1. Configure Device B:

Create VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] quit
```

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign the ports to VLAN 100.

```
[DeviceB] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceB-if-range] port link-type trunk
[DeviceB-if-range] port trunk permit vlan 100
[DeviceB-if-range] quit
```

Create VLAN-interface 100, and assign an IP address to the interface.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ip address 10.0.0.2 24
[DeviceB-Vlan-interface100] quit
```

2. Configure Device C in the same way Device B was configured. (Details not shown.)

Verifying the configuration

Ping Device B from Device A. (Details not shown.)

Verify that GigabitEthernet 1/0/1 on Device A is shut down.

```
[DeviceA] %Dec 11 09:51:06:309 2016 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical
state on the GigabitEthernet1/0/1 changed to down.
%Dec 11 09:51:06:323 2016 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on
the interface GigabitEthernet1/0/1 changed to down.
```

Verify that GigabitEthernet 1/0/1 is shut down because a MAC address move is detected.

```
[DeviceA] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: mac-address moving down
Line protocol state: DOWN
...
```

Verify that GigabitEthernet 1/0/1 comes up automatically after 300 seconds.

```
[DeviceA] %Dec 11 09:56:07:002 2016 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical
state on the GigabitEthernet1/0/1 changed to up.
%Dec 11 09:56:07:004 2016 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on
the interface GigabitEthernet1/0/1 changed to up.
```

Verify that the MAC address of Device B's VLAN-interface 100 moves between GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. You can manually shut down either port to eliminate the loop.

```
[DeviceA] display mac-address mac-move
MAC address    VLAN Current port  Source port   Last time              Times
0000-fc00-6506 100  GE1/0/2       GE1/0/1       2014-12-11 09:29:48    3
0000-fc00-6506 100  GE1/0/1       GE1/0/2       2014-12-11 09:51:03    4

---  2 MAC address moving records found  ---
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
sysname DeviceA
#
mac-address notification mac-move suppression interval 300
mac-address notification mac-move suppression threshold 0
#
vlan 1
#
```

```
vlan 100
#
interface Vlan-interface100
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 mac-address notification mac-move suppression
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device B:

```
#
sysname DeviceB
#
vlan 1
#
vlan 100
#
interface Vlan-interface100
 ip address 10.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device C:

```
#
sysname DeviceC
#
vlan 1
#
vlan 100
#
interface Vlan-interface100
 ip address 10.0.0.3 255.255.255.0
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

Contents

Introduction

This document provides configuration examples of static multicast MAC address entries.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of multicast MAC addresses.

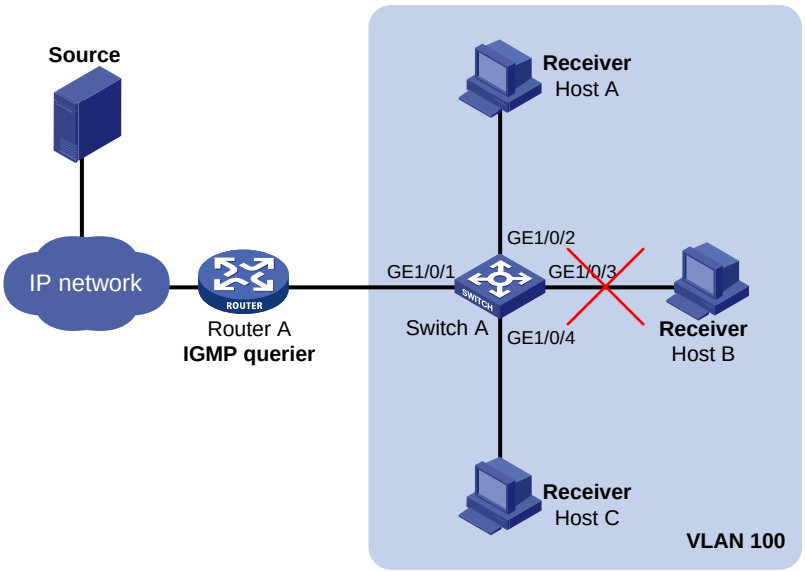
Example: Configuring static multicast MAC address entries

Network configuration

As shown in Figure 1, Router A runs IGMP and acts as the IGMP querier. Switch A does not run a Layer 2 multicast protocol.

Configure a static multicast MAC address entry on Switch A so that only Host A and Host C can receive multicast data for multicast group 224.1.1.1.

Figure 1 Network diagram



Analysis

Multicast MAC address entries guide Layer 2 multicast forwarding. They can be dynamically created through Layer 2 multicast protocols or manually configured by binding multicast MAC addresses and ports.

In this example, Switch A does not run a Layer 2 multicast protocol. To control destination ports of Layer 2 multicast data, configure a static multicast MAC address entry on Switch A.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series	Release 63xx

S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure multicast MAC address entries, follow these guidelines:

- You must specify an unused multicast MAC address in a manually configured multicast MAC address entry.
- By default, Ethernet interfaces, VLAN interfaces, and aggregate interfaces are shut down. You must first use the **undo shutdown** command to bring them up. This example assumes that all these interfaces are already up.

Procedures

On Switch A, create VLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
```

Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to operate in Layer 2 mode, and assign the ports to VLAN 100.

```
[SwitchA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-if-range] port access vlan 100
[SwitchA-if-range] quit
```

Translate the multicast IP address 224.1.1.1 to a multicast MAC address (0100-5e01-0101). (Details not shown.)

Create a static entry for the multicast MAC address 0100-5e01-0101 with GigabitEthernet 1/0/2 and GigabitEthernet 1/0/4 in VLAN 100 as outgoing ports.

```
[SwitchA] mac-address multicast 0100-5e01-0101 interface gigabitethernet 1/0/2
gigabitethernet 1/0/4 vlan 100
```

Verifying the configuration

Display static multicast MAC address entries for VLAN 100 on Switch A.

```
[SwitchA] display mac-address multicast vlan 100
MAC Address      VLAN ID    State           Port/NickName           Aging
0100-5e01-0101   100        Multicast       GE1/0/2                 N
                                            GE1/0/4
```

The output shows that GigabitEthernet 1/0/2 and GigabitEthernet 1/0/4 have become outgoing ports of the multicast MAC group 0100-5e01-0101.

Configuration files

IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 100
#
mac-address multicast 0100-5e01-0101 interface GigabitEthernet1/0/2 GigabitEthernet1/0/4
vlan 100
#
```

Contents

Introduction

This document provides IP unnumbered configuration examples.

This feature enables an interface to borrow an IP address from another interface on the device when the borrowing interface does not have any IP addresses. The borrowing interface is called IP unnumbered interface.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IP unnumbered.

Restrictions and guidelines

When you configure IP unnumbered, follow these restrictions and guidelines:

- Loopback interfaces cannot borrow IP addresses of other interfaces.
- An interface cannot borrow an IP address from an unnumbered interface.
- If an interface has multiple manually configured IP addresses, only the manually configured primary IP address can be borrowed.

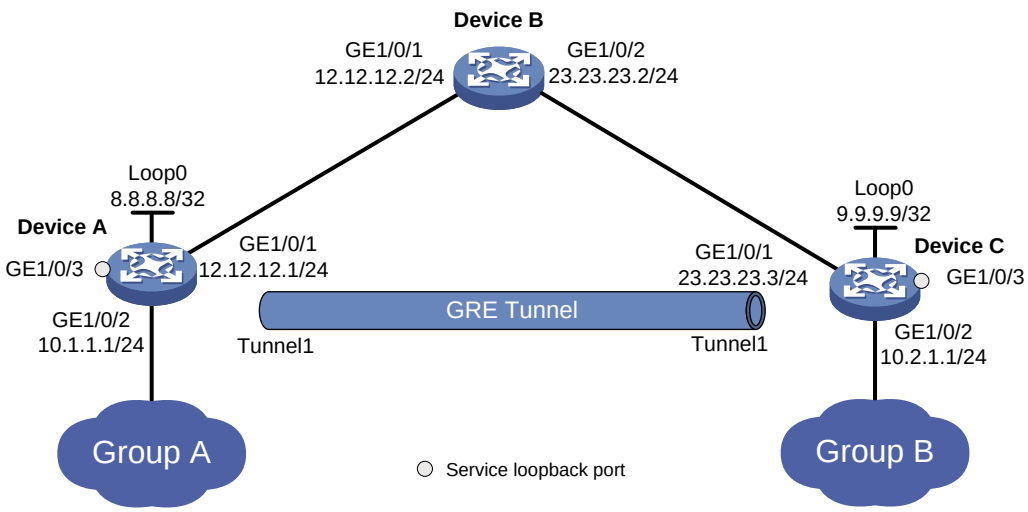
Example: Configuring IP unnumbered

Network configuration

As shown in Figure 1, Group A and Group B are two private IPv4 networks. Device A and Device C will establish a GRE tunnel to interconnect Group 1 and Group 2.

To save IP address space, configure tunnel interface Tunnel 1 to borrow an IP address from the loopback interface loopback 0.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series	Not supported

Hardware	Software version
S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Configuring Device A

1. Assign IP addresses to the interfaces:

   # Assign IP addresses to GigabitEthernet 1/0/1 and loopback 0.

   ```
   <DeviceA> system-view
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] port link-mode route
   [DeviceA-GigabitEthernet1/0/1] ip address 12.12.12.1 24
   [DeviceA-GigabitEthernet1/0/1] quit
   [DeviceA] interface loopback 0
   [DeviceA-LoopBack0] ip address 8.8.8.8 32
   [DeviceA-LoopBack0] quit
   ```

   # Assign IP addresses to other interfaces in the same way an IP address is assigned to GigabitEthernet 1/0/1. (Details not shown.)

2. Configure OSPF:

   # Enable OSPF process 1.

   ```
   [DeviceA] ospf 1
   ```

   # Create Area 0 and specify GigabitEthernet 1/0/1 whose IP address is on network 12.12.12.0/24 to run OSPF in Area 0.

   ```
   [DeviceA-ospf-1] area 0
   [DeviceA-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
   [DeviceA-ospf-1-area-0.0.0.0] quit
   [DeviceA-ospf-1] quit
   ```

3. Configure a GRE tunnel:

   # Create service loopback group 1 and specify the unicast tunnel service for the group.

   ```
   [DeviceA] service-loopback group 1 type tunnel
   ```

   # Assign GigabitEthernet 1/0/3 to the service loopback group.

   ```
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port service-loopback group 1
   [DeviceA-GigabitEthernet1/0/3] quit
   ```

   # Create a tunnel interface Tunnel 1, and specify the tunnel mode as GRE/IPv4.

   ```
   [DeviceA] interface tunnel 1 mode gre
   ```

   # Specify 12.12.12.1 as the source address of interface Tunnel 1.

   ```
   [DeviceA-Tunnel1] source 12.12.12.1
   ```

   # Specify 23.23.23.3 as the destination address of interface Tunnel 1.

   ```
   [DeviceA-Tunnel1] destination 23.23.23.3
   ```

   # Configure interface Tunnel 1 to borrow an IP address from loopback 0.

   ```
   [DeviceA-Tunnel1] ip address unnumbered interface loopback 0
   [DeviceA-Tunnel1] quit
   ```

   # Configure a static route from Device A through the tunnel interface to Group B.

   ```
   [DeviceA] ip route-static 10.2.1.0 255.255.255.0 tunnel 1
   ```

Configuring Device B

1. Assign IP addresses to the interfaces:

   # Assign an IP address to GigabitEthernet 1/0/1.

   ```
   <DeviceB> system-view
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] port link-mode route
   [DeviceB-GigabitEthernet1/0/1] ip address 12.12.12.2 24
   [DeviceB-GigabitEthernet1/0/1] quit
   ```

   # Assign an IP address to GigabitEthernet 1/0/2 in the same way an IP address is assigned to GigabitEthernet 1/0/1. (Details not shown.)

2. Configure OSPF:

   # Enable OSPF process 1.

   ```
   [DeviceB] ospf 1
   ```

   # Create Area 0 and specify GigabitEthernet 1/0/1 whose IP address is on network 12.12.12.0/24 to run OSPF in Area 0.

   ```
   [DeviceB-ospf-1] area 0
   [DeviceB-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
   ```

   # Create Area 0 and specify GigabitEthernet 1/0/2 whose IP address is on network 23.23.23.0/24 to run OSPF in Area 0.

   ```
   [DeviceB-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
   [DeviceB-ospf-1-area-0.0.0.0] quit
   [DeviceB-ospf-1] quit
   ```

Configuring Device C

1. Assign IP addresses to the interfaces:

   # Assign IP addresses to GigabitEthernet 1/0/1 and loopback 0.

   ```
   <DeviceC> system-view
   [DeviceC] interface gigabitethernet 1/0/1
   [DeviceC-GigabitEthernet1/0/1] port link-mode route
   [DeviceC-GigabitEthernet1/0/1] ip address 23.23.23.3 24
   [DeviceC-GigabitEthernet1/0/1] quit
   [DeviceC] interface loopback 0
   [DeviceC-LoopBack0] ip address 9.9.9.9 32
   [DeviceC-LoopBack0] quit
   ```

   # Assign IP addresses to other interfaces in the same way an IP address is assigned to GigabitEthernet 1/0/1. (Details not shown.)

2. Configure OSPF:

   # Enable OSPF process 1.

   ```
   [DeviceC] ospf 1
   ```

   # Create Area 0 and specify GigabitEthernet 1/0/1 whose IP address is on network 23.23.23.0/24 to run OSPF in Area 0.

   ```
   [DeviceC-ospf-1] area 0
   [DeviceC-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
   [DeviceC-ospf-1-area-0.0.0.0] quit
   [DeviceC-ospf-1] quit
   ```

3. Configure a GRE tunnel:

Create service loopback group 1 and specify the unicast tunnel service for the group.

```
[DeviceC] service-loopback group 1 type tunnel
```

Assign GigabitEthernet 1/0/3 to the service loopback group.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port service-loopback group 1
[DeviceC-GigabitEthernet1/0/3] quit
```

Create a tunnel interface Tunnel 1, and specify the tunnel mode as GRE/IPv4.

```
[DeviceC] interface tunnel 1 mode gre
```

Specify 23.23.23.3 as the source address of interface Tunnel 1.

```
[DeviceC-Tunnel1] source 23.23.23.3
```

Specify 12.12.12.1 as the destination address of interface Tunnel 1.

```
[DeviceC-Tunnel1] destination 12.12.12.1
```

Configure interface Tunnel 1 to borrow an IP address from loopback 0.

```
[DeviceC-Tunnel1] ip address unnumbered interface loopback 0
[DeviceC-Tunnel1] quit
```

Configure a static route from Device C through the tunnel interface to Group A.

```
[DeviceC] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

Verifying the configuration

This example uses Device A to verify the configuration.

Verify that the interface Tunnel 1 has borrowed the IP address 8.8.8.8/32 from loopback 0.

```
[DeviceA] display interface tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 1476
Internet Address: 8.8.8.8/32 (Unnumbered)
Tunnel source 12.12.12.1, destination 23.23.23.3
Tunnel keepalive disabled
Tunnel TTL 255
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 11 packets, 924 bytes, 0 drops
Output: 10 packets, 840 bytes, 0 drops
```

Verify that GigabitEthernet 1/0/2 on Device A can ping the IP address of GigabitEthernet 1/0/2 on Device C.

Verify that VLAN-interface 10 on Device A can ping the IP address of VLAN-interface 10 on Device C.

```
[DeviceA] ping -a 10.1.1.1 10.2.1.1
Ping 10.2.1.1 (10.2.1.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.2.1.1: icmp_seq=0 ttl=255 time=32.641 ms
56 bytes from 10.2.1.1: icmp_seq=1 ttl=255 time=4.881 ms
56 bytes from 10.2.1.1: icmp_seq=2 ttl=255 time=4.816 ms
56 bytes from 10.2.1.1: icmp_seq=3 ttl=255 time=26.393 ms
56 bytes from 10.2.1.1: icmp_seq=4 ttl=255 time=43.003 ms

--- Ping statistics for 10.2.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.816/22.347/43.003/15.241 ms
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 service-loopback group 1 type tunnel
#
ospf 1
 area 0.0.0.0
  network 12.12.12.0 0.0.0.255
#
vlan 10
#
vlan 12
#
interface LoopBack0
 ip address 8.8.8.8 255.255.255.255
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
```

```
interface Tunnel1 mode gre
 ip address unnumbered interface LoopBack0
 source 12.12.12.1
 destination 23.23.23.3
#
 ip route-static 10.2.1.0 24 Tunnel1
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
vlan 12
#
vlan 23
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.12.12.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 23.23.23.2 255.255.255.0
#
```

- Device C:

```
#
 service-loopback group 1 type tunnel
#
ospf 1
 area 0.0.0.0
  network 23.23.23.0 0.0.0.255
#
vlan 10
#
vlan 23
#
interface LoopBack0
 ip address 9.9.9.9 255.255.255.255
#
interface Vlan-interface10
```

```
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 23.23.23.3 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode gre
 ip address unnumbered interface LoopBack0
 source 23.23.23.3
 destination 12.12.12.1
#
 ip route-static 10.1.1.0 24 Tunnel1
#
```

Contents

Introduction

This document provides MVRP configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MVRP.

Example: Configuring MVRP

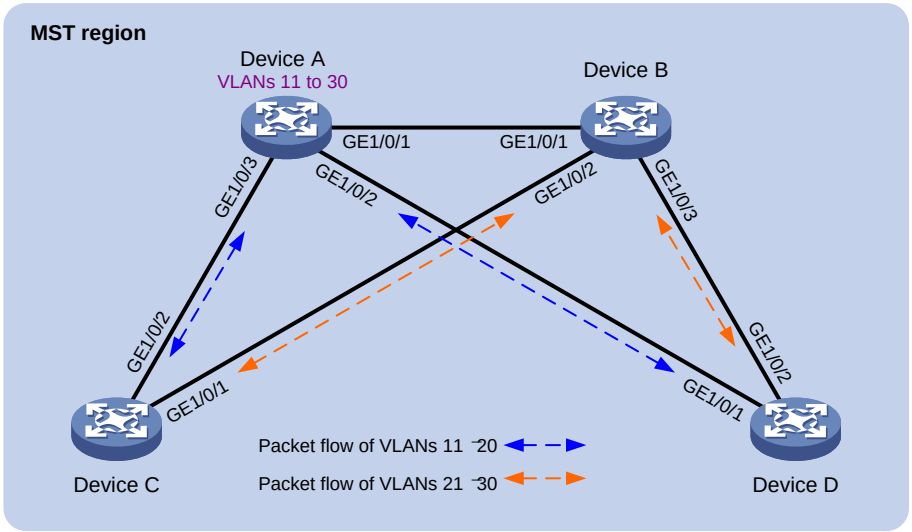
Network configuration

As shown in Figure 1:

- Device A and Device B are core layer devices. Device C and Device D are aggregation layer devices.
- Ports on all devices allow packets from VLANs 11 through 30 to pass through.
- MSTP implements load balancing and link backup for traffic of VLANs 11 through 30 between the core layer devices and the aggregation layer devices.

Configure MVRP on all devices to synchronize and update VLAN information. When the network is stable, set the registration mode to **fixed** on GigabitEthernet 1/0/1 of Device B to maintain dynamic VLAN information.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To assign all devices to the same MST region, configure the same settings for the following parameters on all the devices:
  - Spanning tree mode. (This example uses the default mode MSTP.)
  - MST region name. (This example uses the region name **test**.)
  - MST region revision level. (This example uses the default setting 0.)
  - VLAN-to-instance mappings. (This example maps VLANs 11 through 20 to MSTI 1, and maps VLANs 21 through 30 to MSTI 2.)
- For MSTIs 1 and 2 to use different uplinks for backup, set Device A and Device B as the root bridges of MSTIs 1 and 2, respectively.
- Make sure each MSTI is mapped to an existing VLAN on each device in the network.
- MVRP takes effect only on trunk ports. You must set the port link type to trunk for MVRP participants.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI switch and S5500V3-48P-SI switch)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI switch, S5120V3-28P-HPWR-SI switch, and S5120V3-54P-PWR-SI switch)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx

WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure MVRP, follow these restrictions and guidelines:

- MVRP can work with STP, RSTP, or MSTP. Ports blocked by STP, RSTP, or MSTP can receive and send MVRP frames. MVRP cannot work with other link layer topology protocols, including service loopback, PVST, RRPP, and Smart Link.
- On a Layer 2 aggregate interface, MVRP takes effect on both the aggregate interface and all Selected member ports in the link aggregation group.
- MVRP configuration made on an aggregation group member port takes effect only after the port is removed from the aggregation group.

Procedures

Configuring Device A

Create VLANs 11 through 30.

```
<DeviceA> system-view
[DeviceA] vlan 11 to 30
```

Enter MST region view.

```
[DeviceA] stp region-configuration
```

Set the MST region name to **test**.

```
[DeviceA-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1.

```
[DeviceA-mst-region] instance 1 vlan 11 to 20
```

Map VLANs 21 through 30 to MSTI 2.

```
[DeviceA-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure Device A as the root bridge of MSTI 1.

```
[DeviceA] stp instance 1 root primary
```

Enable the spanning tree feature globally.

```
[DeviceA] stp global enable
```

Enable MVRP globally.

```
[DeviceA] mvrp global enable
```

Configure the ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as trunk ports, assign the ports to VLANs 11 through 30, and enable MVRP on these ports.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-mode bridge
[DeviceA-if-range] port link-type trunk
[DeviceA-if-range] port trunk permit vlan 11 to 30
[DeviceA-if-range] mvrp enable
[DeviceA-if-range] undo shutdown
[DeviceA-if-range] quit
```

Configuring Device B

Create VLANs 11 and 21.

```
<DeviceB> system-view
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 21
[DeviceB-vlan21] quit
```

Enter MST region view.

```
[DeviceB] stp region-configuration
```

Set the MST region name to **test**.

```
[DeviceB-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1.

```
[DeviceB-mst-region] instance 1 vlan 11 to 20
```

Map VLANs 21 through 30 to MSTI 2.

```
[DeviceB-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure Device B as the root bridge of MSTI 2.

```
[DeviceB] stp instance 2 root primary
```

Enable the spanning tree feature globally.

```
[DeviceB] stp global enable
```

Enable MVRP globally.

```
[DeviceB] mvrp global enable
```

Configure the ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as trunk ports, assign the ports to VLANs 11 through 30, and enable MVRP on these ports.

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceB-if-range] port link-mode bridge
[DeviceB-if-range] port link-type trunk
[DeviceB-if-range] port trunk permit vlan 11 to 30
[DeviceB-if-range] mvrp enable
[DeviceB-if-range] undo shutdown
[DeviceB-if-range] quit
```

Configuring Device C

Create VLANs 11 and 21.

```
<DeviceC> system-view
[DeviceC] vlan 11
[DeviceC-vlan11] quit
[DeviceC] vlan 21
[DeviceC-vlan21] quit
```

Enter MST region view.

```
[DeviceC] stp region-configuration
```

Set the MST region name to **test**.

```
[DeviceC-mst-region] region-name test
```

Map VLANs 11 through 20 to MSTI 1.

```
[DeviceC-mst-region] instance 1 vlan 11 to 20
```

Map VLANs 21 through 30 to MSTI 2.

```
[DeviceC-mst-region] instance 2 vlan 21 to 30
```

Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Enable the spanning tree feature globally.

```
[DeviceC] stp global enable
```

Enable MVRP globally.

```
[DeviceC] mvrp global enable
```

Configure the ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, assign the ports to VLANs 11 through 30, and enable MVRP on these ports.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-mode bridge
[DeviceC-if-range] port link-type trunk
[DeviceC-if-range] port trunk permit vlan 11 to 30
[DeviceC-if-range] mvrp enable
[DeviceC-if-range] undo shutdown
[DeviceC-if-range] quit
```

Configuring Device D

Configure Device D in the same way Device C is configured. (Details not shown.)

Verifying the configuration

Verifying MSTI topologies

Display brief spanning tree information on Device A.

```
[DeviceA] display stp brief
 MST ID   Port                                Role  STP State   Protection
...
 1        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
```

```
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
```

Display brief spanning tree information on Device B.

```
[DeviceB] display stp brief
 MST ID   Port                                Role  STP State   Protection
...
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
```

Display brief spanning tree information on Device C.

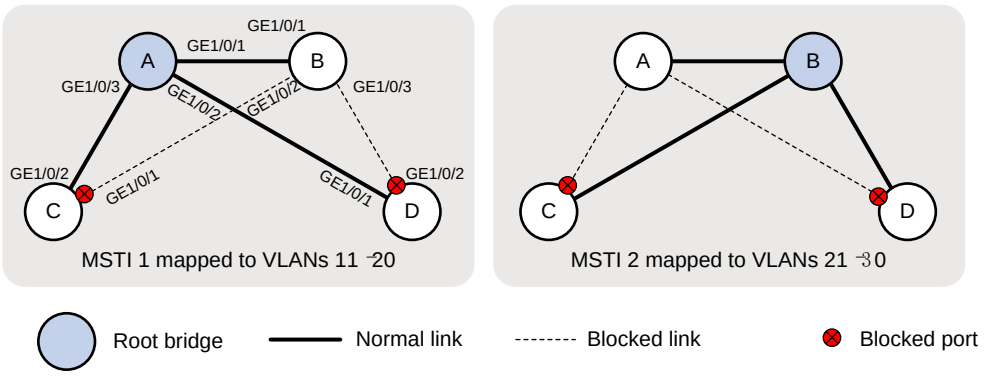
```
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
...
 1        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MST ID   Port                                Role  STP State   Protection
...
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

Based on the output, you can get MSTI topologies, as shown in Figure 2.

Figure 2 MSTI topologies



Verifying local VLAN information on all devices

Display local VLAN information on Device A.

```
[DeviceA] display mvrp running-status
 -------[MVRP Global Info] -------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11, 21
 Declared VLANs :
  1(default), 11-30
 Propagated VLANs :
  1(default), 11, 21

 ----[GigabitEthernet1/0/2] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11
 Declared VLANs :
  1(default), 11-30
 Propagated VLANs :
  1(default), 11

 ----[GigabitEthernet1/0/3] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11
```

```
 Declared VLANs :
  1(default), 11-30
 Propagated VLANs :
  1(default), 11
```

The output shows that all ports of Device A have declared VLANs 11 through 30.

Display local VLAN information on Device B.

```
[DeviceB] display mvrp running-status
 -------[MVRP Global Info] -------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11-30
 Declared VLANs :
  1(default), 11, 21
 Propagated VLANs :
  1(default), 11-30

 ----[GigabitEthernet1/0/2] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  21
 Declared VLANs :
  1(default), 11-30
 Propagated VLANs :
  21

 ----[GigabitEthernet1/0/3] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
```

```
 Registration Type              : Normal
 Registered VLANs :
  21
 Declared VLANs :
  1(default), 11-30
 Propagated VLANs :
  21
```

The output shows that:

- GigabitEthernet 1/0/1 has registered and propagated VLANs 11 through 30.
- GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 have declared VLANs 11 through 30.

Display local VLAN information on Device C.

```
[DeviceC] display mvrp running-status
 -------[MVRP Global Info] -------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11-30
 Declared VLANs :
  21
 Propagated VLANs :
  21-30

 ----[GigabitEthernet1/0/2] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11-30
 Declared VLANs :
  1(default), 11
 Propagated VLANs :
  1(default), 11-20
```

The output shows that:

- GigabitEthernet 1/0/1 has registered VLANs 11 through 30. Because GigabitEthernet 1/0/1 is a blocked port in MSTI 1, the port propagated only VLANs 21 through 30.
- GigabitEthernet 1/0/2 has registered VLANs 11 through 30. Because GigabitEthernet 1/0/2 is a blocked port in MSTI 2, the port propagated only VLANs 11 through 20.

Display local VLAN information on Device D.

```
[DeviceD] display mvrp running-status
 -------[MVRP Global Info] -------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11-30
 Declared VLANs :
  1(default), 11
 Propagated VLANs :
  1(default), 11-20

 ----[GigabitEthernet1/0/2] ----
 Config  Status                 : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Normal
 Registered VLANs :
  1(default), 11-30
 Declared VLANs :
  21
 Propagated VLANs :
  21-30
```

The output shows that:

- GigabitEthernet 1/0/1 has registered VLANs 11 through 30. Because GigabitEthernet 1/0/1 is a blocked port in MSTI 2, the port propagated only VLANs 11 through 20.
- GigabitEthernet 1/0/2 has registered VLANs 11 through 30. Because GigabitEthernet 1/0/2 is a blocked port in MSTI 1, the port propagated only VLANs 21 through 30.

Verifying VLAN information after changing the registration mode

When the network is stable, set the MVRP registration mode to **fixed** on GigabitEthernet 1/0/1 of Device B. Then, verify that dynamic VLANs on the port will not be deregistered.

Set the MVRP registration mode to **fixed** on GigabitEthernet 1/0/1 of Device B.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] mvrp registration fixed
[DeviceB-GigabitEthernet1/0/1] quit
```

Remove VLAN 30 from Device A.

```
[DeviceA] undo vlan 30
```

Display local VLAN information on GigabitEthernet 1/0/1 of Device B.

```
[DeviceB] display mvrp running-status interface gigabitethernet 1/0/1
 -------[MVRP Global Info] -------
 Global Status     : Enabled
 Compliance-GVRP   : False

 ----[GigabitEthernet1/0/1] ----
 Config Status                  : Enabled
 Running Status                 : Enabled
 Join Timer                     : 20 (centiseconds)
 Leave Timer                    : 60 (centiseconds)
 Periodic Timer                 : 100 (centiseconds)
 LeaveAll Timer                 : 1000 (centiseconds)
 Registration Type              : Fixed
 Registered VLANs :
  1(default), 21-30
 Declared VLANs :
  1(default), 21
 Propagated VLANs :
  1(default), 21-30
```

The output shows that VLAN information on GigabitEthernet 1/0/1 does not change after you set its MVRP registration mode to **fixed**.

Create VLAN 30 on Device A.

```
[DeviceA] vlan 30
```

Verifying VLAN information after changing the network topology

Shut down GigabitEthernet1/0/2 of Device C to change the network topology, and then verify the VLAN information on this port.

Display VLAN information on GigabitEthernet 1/0/2 of Device C.

```
[DeviceC] display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2
Current state: UP
Line protocol state: UP
```

```
...
Port link-type: Trunk
 VLAN Passing:   1(default vlan), 11-30
 VLAN permitted: 1(default vlan), 11-30
 Trunk port encapsulation: IEEE 802.1q
...
```

The output shows that VLAN 1 and VLANs 11 through 30 can pass through GigabitEthernet 1/0/2.

Shut down GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Display brief spanning tree information on Device C.

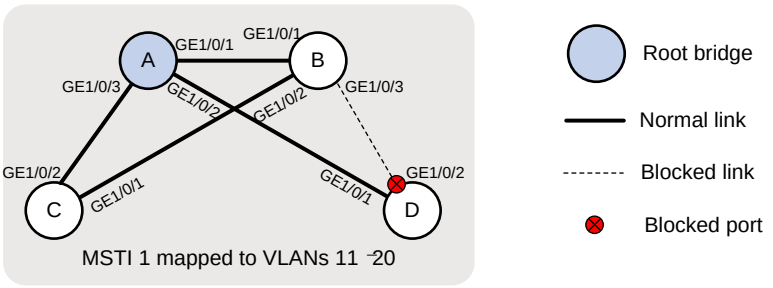
```
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
```

Display brief spanning tree information on Device D.

```
[DeviceD] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 2        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

Based on the output, you can get the topology of MSTI 1, as shown in Figure 3.

Figure 3 Topology of MSTI 1



Display dynamic VLANs on Device C.

```
[DeviceC] display vlan dynamic
 Dynamic VLANs: 18
 The dynamic VLANs include:
 12-20, 22-30
```

Display VLAN information on GigabitEthernet 1/0/2 of Device C.

```
[DeviceC] display interface gigabitethernet 1/0/2
...
Port link-type: Trunk
```

```
 VLAN Passing:   1(default vlan), 11, 21
 VLAN permitted: 1(default vlan), 11-30
 Trunk port encapsulation: IEEE 802.1q
...
```

The output shows that:

- VLANs 1, 11, and 21 can pass through GigabitEthernet 1/0/2.
- GigabitEthernet 1/0/2 failed to learn dynamic VLANs.

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
 mvrp global enable
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 to 1 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
```

- Device B:

```
#
 sysname DeviceB
#
 mvrp global enable
#
vlan 1
#
vlan 11
#
vlan 21
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 2 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
```

- Device C:

```
#
 sysname DeviceC
#
 mvrp global enable
#
```

```
vlan 1
#
vlan 11
#
vlan 21
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
```

- Device D:

```
#
 sysname DeviceD
#
 mvrp global enable
#
vlan 1
#
vlan 11
#
vlan 21
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
 mvrp enable
#
```

Contents

Introduction

This document provides examples for configuring the MCE to advertise VPN routes to the PE.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MCE.

Example: Configuring the MCE to advertise VPN routes to the PE by using OSPF

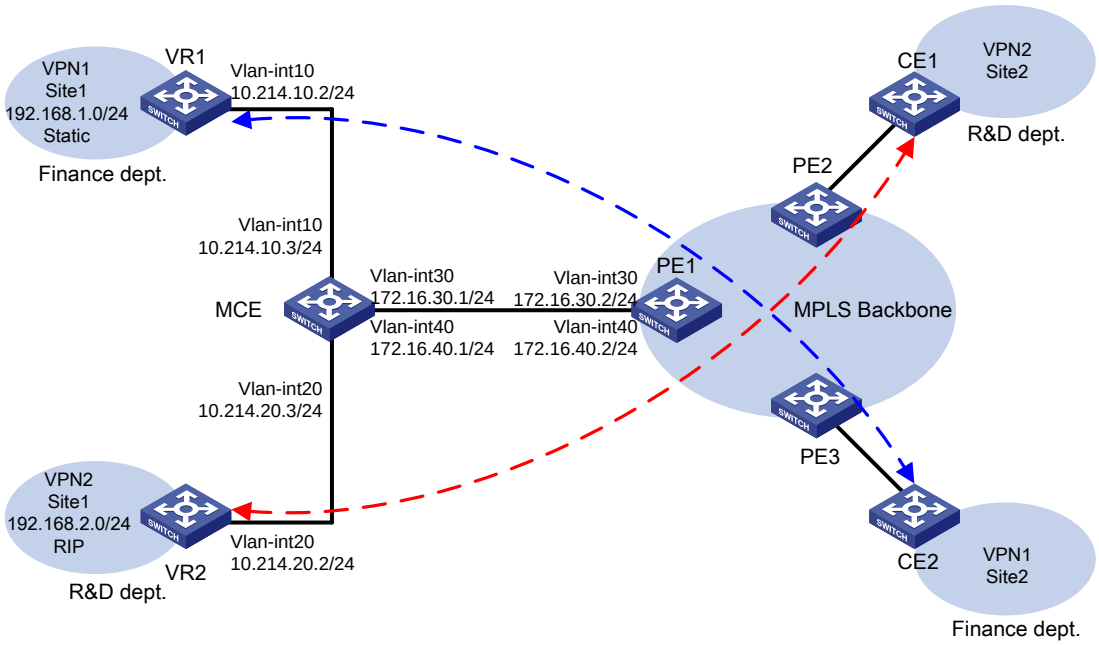
Network configuration

As shown in Figure 1, an enterprise has two MPLS L3VPNs. VPN 1 for the finance department uses static routes, and VPN 2 for the R&D department uses RIP routes. Site 1 of VPN 1 and Site 1 of VPN 2 are connected to the MPLS backbone through the same CE device (MCE). Site 2 of VPN 1 and Site 2 of VPN 2 are connected to the MPLS backbone through separate CEs (CE 1 and CE 2).

Configure the MCE to allow communication between the local and remote sites of the same VPN and isolate access between sites of different VPNs.

Configure the MCE and PE 1 to use OSPF to exchange VPN routes.

Figure 1 Network diagram

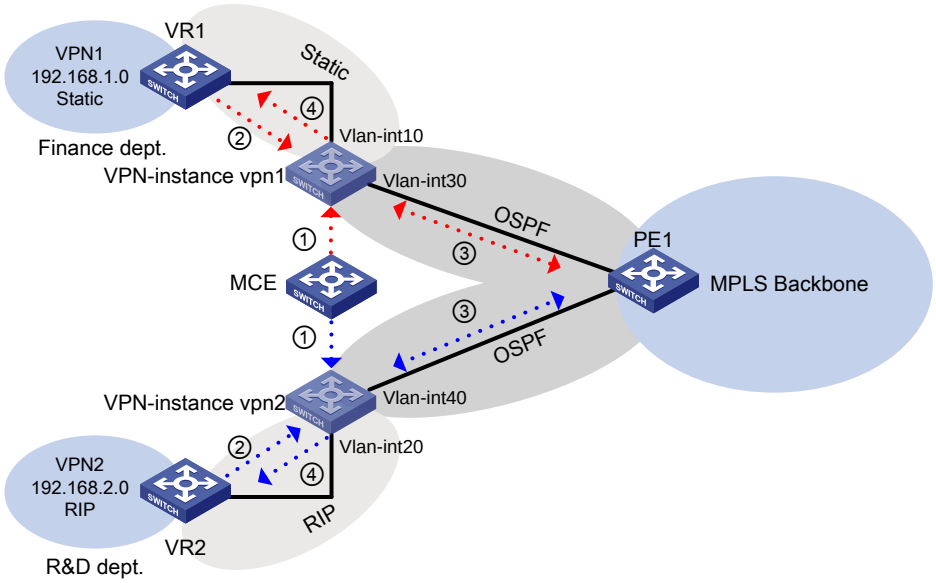


Analysis

To meet the network requirements, you must perform the following tasks:

1. Create VPN instances on the MCE and PE 1, and bind each VPN instance to the interfaces that need to forward data for that VPN instance.
2. Redistribute the VPN routes to the routing table of the corresponding VPN instance.
3. Advertise the VPN routes to PE 1 through OSPF, and receive remote VPN routes from PE 1.
4. Redistribute the remote VPN routes to the local VPN sites.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except forS5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series	Release 63xx

Hardware	Software version
S5130S-SI switch series	
S5130S-LI switch series	Not supported
S5120V2-SI switch series	Release 63xx
S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except for S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series	Release 63xx
S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx

Hardware	Software version
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

Follow these restrictions and guidelines when you configure the MCE to advertise VPN routes to the PE by using OSPF:

- Associating an interface with a VPN instance by using the **ip binding vpn-instance** command deletes the IP address of the interface. You must reconfigure the interface's IP address after the association.
- An OSPF process can belong to only one VPN instance, but a VPN instance can use multiple OSPF processes to advertise private routes. The OSPF processes in a VPN instance must have the same domain ID to ensure correct route advertisement.

Procedures

This example provides only the configurations on the MCE, VR 1, VR 2, and PE 1. Configurations on other devices are not shown.

1. Configure VPN instances on the MCE and PE 1:

On the MCE, create a VPN instance named **vpn1**, and configure its RD as 10:1.

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
```

Create a VPN instance named **vpn2**, and configure its RD as 20:1.

```
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
```

Bind VLAN-interface 10 to the VPN instance **vpn1**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
[MCE-Vlan-interface10] ip address 10.214.10.3 24
[MCE-Vlan-interface10] quit
[MCE-Vlan-interface10] quit
```

Bind VLAN-interface 20 to the VPN instance **vpn2**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

Bind VLAN-interface 30 to the VPN instance **vpn1**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit
```

Bind VLAN-interface 40 to the VPN instance **vpn2**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE 1, create VPN instances **vpn1** and **vpn2**, and configure RDs for the VPN instances. Make sure the RDs are the same as those configured on the MCE.

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 20:1
[PE1-vpn-instance-vpn2] quit
```

Bind VLAN-interface 30 to the VPN instance **vpn1** and VLAN-interface 40 to the VPN instance **vpn2**, and configure IP addresses for the interfaces.

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ip address 172.16.30.2 24
[PE1-Vlan-interface30] quit
[PE1] interface vlan-interface 40
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
[PE1-Vlan-interface40] ip address 172.16.40.2 24
[PE1-Vlan-interface40] quit
```

2. Configure routing between the MCE and VPN sites:

On VR 1, assign IP address 10.214.10.2/24 to the interface connected to the MCE. (Details not shown.)

On VR 1, configure a default route with the next hop as the MCE.

```
<VR1> system-view
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

On the MCE, configure a static route to 192.168.1.0/24 with the next hop 10.214.10.2, and bind the static route to the VPN instance **vpn1**.

```
[MCE] ip route-static vpn-instance vpn1 192.168.1.0 24 10.214.10.2
```

On the MCE, display the routing table for the VPN instance **vpn1**.

```
[MCE] display ip routing-table vpn-instance vpn1

Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.214.10.0/24      Direct 0     0           10.214.10.3     Vlan10
10.214.10.3/32      Direct 0     0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0     0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0     0           127.0.0.1       InLoop0
172.16.30.0/24      Direct 0     0           172.16.30.1     Vlan30
172.16.30.1/32      Direct 0     0           127.0.0.1       InLoop0
192.168.1.0/24      Static 60    0           10.214.10.2     Vlan10
```

The output shows that the MCE has a static route for the VPN instance **vpn1**.

On VR 2, assign IP address 10.214.20.2/24 to the interface connected to the MCE. (Details not shown.)

On VR 2, enable RIP process 20 to advertise networks 192.168.2.0/24 and 10.214.20.0/24, and disable route summarization.

```
<VR2> system-view
[VR2] rip 20
[VR2-rip-20] network 192.168.2.0
[VR2-rip-20] network 10.0.0.0
[VR2-rip-20] undo summary
```

On the MCE, enable RIP process 20 for the VPN instance **vpn2** to exchange routes with VPN 2 site 1.

```
[MCE] rip 20 vpn-instance vpn2
```

On the MCE, advertise the network 10.214.20.0 and disable route summarization.

```
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] undo summary
```

On the MCE, redistribute OSPF routes.

```
[MCE-rip-20] import-route ospf 20
[MCE-rip-20] quit
```

On the MCE, display the routing table for the VPN instance **vpn2**.

```
[MCE] display ip routing-table vpn-instance vpn2

Destinations : 5        Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.214.20.0/24      Direct 0    0            10.214.20.3     Vlan20
10.214.20.3/32      Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
172.16.40.0/30      Direct 0    0            172.16.40.1     Vlan40
172.16.40.1/32      Direct 0    0            127.0.0.1       InLoop0
192.168.2.0/24      RIP    100  1            10.214.20.2     Vlan20
```

The output shows that the MCE has learned a RIP route to VPN 2, which is in a different routing table from the static route to VPN 1. The routes from different VPNs are separated.

3. Configure routing between the MCE and PE 1:

On the MCE, bind Loopback 0 to the VPN instance **vpn1** and configure an IP address for the loopback interface.

```
[MCE] interface Loopback 0
[MCE-Loopback0] ip binding vpn-instance vpn1
[MCE-Loopback0] ip address 100.100.10.1 32
[MCE-Loopback0] quit
```

On PE 1, bind Loopback 0 to the VPN instance **vpn1** and configure an IP address for the loopback interface.

```
[PE1] interface Loopback 0
[PE1-Loopback0] ip binding vpn-instance vpn1
[PE1-Loopback0] ip address 100.100.11.1 32
[PE1-Loopback0] quit
```

On the MCE, enable OSPF process 10, specify the router ID as the IP address of Loopback 0, and bind the process to the VPN instance **vpn1**.

```
[MCE] ospf 10 router-id 100.100.10.1 vpn-instance vpn1
```

Disable routing loop detection for OSPF process 10.

```
[MCE-ospf-10] vpn-instance-capability simple
```

Advertise the network 172.16.30.0/24 in area 0, and redistribute the static route of VPN 1.

```
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 172.16.30.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
[MCE-ospf-10] quit
```

On PE 1, enable OSPF process 10, specify the router ID as the IP address of Loopback 0, and bind the process to the VPN instance **vpn1**.

```
[PE1] ospf 10 router-id 100.100.11.1 vpn-instance vpn1
```

Set the domain ID to 10.

```
[PE1-ospf-10] domain-id 10
```

Disable routing loop detection for OSPF process 10.

```
[PE1-ospf-10] vpn-instance-capability simple
```

Advertise the network 172.16.30.0/24 in area 0.

```
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 172.16.30.0 0.0.0.255
```

On the MCE, bind Loopback 1 to the VPN instance **vpn2** and configure an IP address for the loopback interface.

```
[MCE] interface Loopback 1
[MCE-Loopback1] ip binding vpn-instance vpn2
[MCE-Loopback1] ip address 100.100.20.1 32
```

On PE 1, bind Loopback 1 to the VPN instance **vpn2** and configure an IP address for the loopback interface.

```
[PE1] interface Loopback 1
[PE1-Loopback1] ip binding vpn-instance vpn2
[PE1-Loopback1] ip address 100.100.21.1 32
```

On the MCE, enable OSPF process 20, specify the router ID as the IP address of Loopback 1, and bind the process to the VPN instance **vpn2**.

```
[MCE] ospf 20 router-id 100.100.20.1 vpn-instance vpn2
```

Disable routing loop detection for OSPF process 20.

```
[MCE-ospf-20] vpn-instance-capability simple
```

Advertise the network 172.16.40.0/24 in area 0, and redistribute the RIP route of VPN 2.

```
[MCE-ospf-20] area 0
[MCE-ospf-20-area-0.0.0.0] network 172.16.40.0 0.0.0.255
[MCE-ospf-20-area-0.0.0.0] quit
[MCE-ospf-20] import-route rip 20
```

On PE 1, enable OSPF process 20, specify the router ID as the IP address of Loopback 1, and bind the process to the VPN instance **vpn2**.

```
[PE1] ospf 20 router-id 100.100.21.1 vpn-instance vpn2
```

Set the domain ID to 20.

```
[PE1-ospf-20] domain-id 20
```

Disable routing loop detection for OSPF process 20.

```
[PE1-ospf-20] vpn-instance-capability simple
```

Advertise the network 172.16.40.0/24 in area 0.

```
[PE1-ospf-20] area 0
[PE1-ospf-20-area-0.0.0.0] network 172.16.40.0 0.0.0.255
[PE1-ospf-20-area-0.0.0.0] quit
```

```
[PE1-ospf-20] quit
```

Verifying the configuration

Verify that PE 1 has learned the static route of VPN 1 through OSPF.

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
100.100.11.1/32     Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.30.0/24      Direct  0   0           172.16.30.2     Vlan30
172.16.30.0/32      Direct  0   0           172.16.30.2     Vlan30
172.16.30.2/32      Direct  0   0           127.0.0.1       InLoop0
172.16.30.255/32    Direct  0   0           172.16.30.2     Vlan30
192.168.1.0/24      O_INTRA 150 1           172.16.30.1     Vlan30
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

Verify that PE 1 has learned the RIP route of VPN 2 through OSPF.

```
[PE1] display ip routing-table vpn-instance vpn2

Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
100.100.21.1/32     Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.40.0/24      Direct  0   0           172.16.40.2     Vlan40
172.16.40.0/32      Direct  0   0           172.16.40.2     Vlan40
172.16.40.2/32      Direct  0   0           127.0.0.1       InLoop0
172.16.40.255/32    Direct  0   0           172.16.40.2     Vlan40
192.168.2.0/24      O_INTRA 150 1           172.16.40.1     Vlan40
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- VR 1:

```
#
 vlan 10
#
interface Vlan-interface10
 ip address 10.214.10.2 255.255.255.0
#
 ip route-static 0.0.0.0 0 10.214.10.3
#
```

- VR 2:

```
#
rip 20
 network 10.0.0.0
 network 192.168.2.0
#
 vlan 20
#
interface Vlan-interface20
 ip address 10.214.20.2 255.255.255.0
#
```

- MCE:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
ospf 10 router-id 100.100.10.1 vpn-instance vpn1
 import-route static
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.30.0 0.0.0.255
#
ospf 20 router-id 100.100.20.1 vpn-instance vpn2
 import-route rip 20
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.40.0 0.0.0.255
#
rip 20 vpn-instance vpn2
 undo summary
```

```
 network 10.0.0.0
 import-route ospf 20
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.10.1 255.255.255.255
#
interface LoopBack1
 ip binding vpn-instance vpn2
 ip address 100.100.20.1 255.255.255.255
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.1 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.1 255.255.255.0
#
 ip route-static vpn-instance vpn1 192.168.1.0 255.255.255.0 10.214.10.2
#
```

- PE 1:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
ospf 10 router-id 100.100.10.1 vpn-instance vpn1
 domain-id 0.0.0.10
 vpn-instance-capability simple
```

```
 area 0.0.0.0
  network 172.16.30.0 0.0.0.255
#
ospf 20 router-id 100.100.20.1 vpn-instance vpn2
 domain-id 0.0.0.20
 vpn-instance-capability simple
 area 0.0.0.0
  network 172.16.40.0 0.0.0.255
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.11.1 255.255.255.255
#
interface LoopBack1
 ip binding vpn-instance vpn2
 ip address 100.100.21.1 255.255.255.255
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.2 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.2 255.255.255.0
#
```

Example: Configuring the MCE to advertise VPN routes to the PE by using BGP

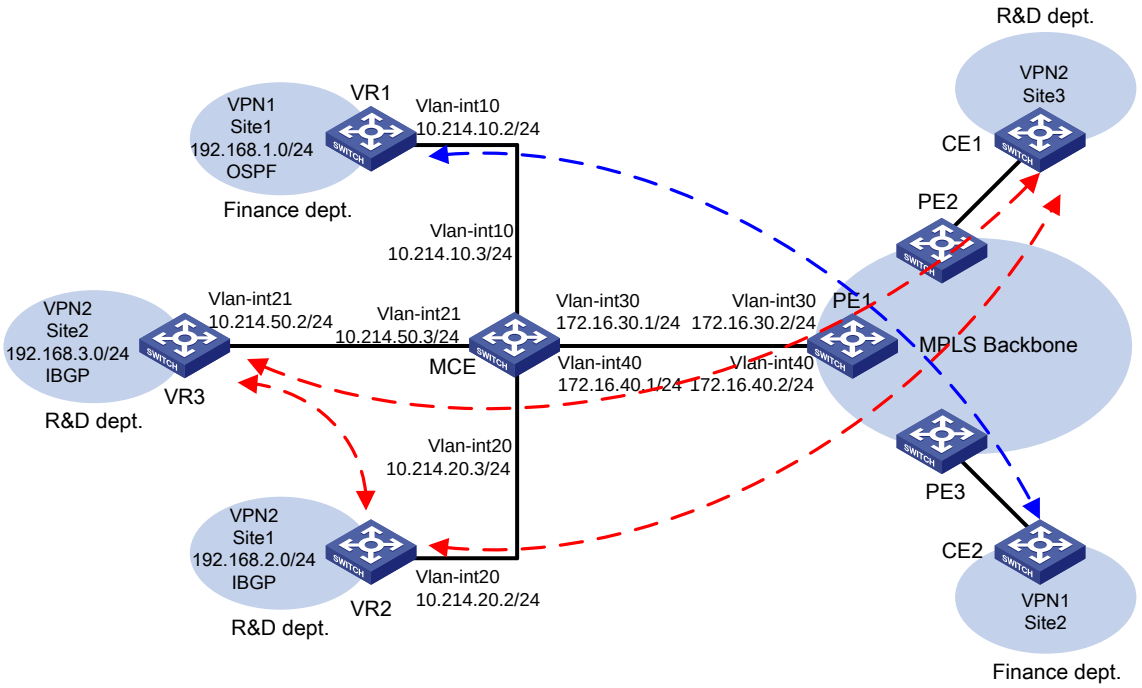
Network configuration

As shown in Figure 3, an enterprise has two MPLS L3VPNs. VPN 1 for the finance department uses OSPF, and VPN 2 for the R&D department uses IBGP. Site 1 of VPN 1, Site 2 of VPN 2, and Site 1 of VPN 2 are connected to the MPLS backbone through the same CE device (MCE). Site 3 of VPN 2 and Site 2 of VPN 1 are connected to the MPLS backbone through separate CEs (CE 1 and CE 2).

Configure the MCE to allow communication between the local and remote sites of the same VPN and isolate access between sites of different VPNs.

Configure the MCE and PE 1 to use BGP to exchange VPN routes.

Figure 3 Network diagram



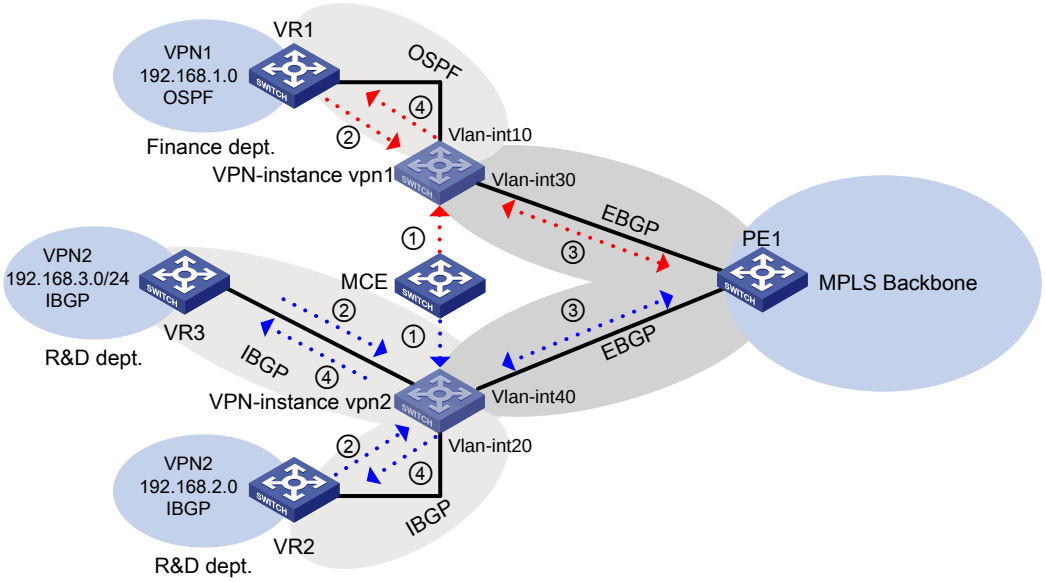
Analysis

To meet the network requirements, you must perform the following tasks:

1. Create VPN instances on the MCE and PE 1, and bind each VPN instance to the interfaces that need to forward data for that VPN instance.
2. Redistribute the VPN routes to the routing table of the corresponding VPN instance.

   IBGP requires a fully meshed network or a router reflector. In this example, you must configure the MCE as the IBGP route reflector.
3. Advertise the VPN routes to PE 1 through EBGP, and receive remote VPN routes from PE 1.
4. Redistribute the remote VPN routes to the local VPN sites.

Figure 4 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except for S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except for S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch	Not supported

Hardware	Software version
E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

Associating an interface with a VPN instance by using the **ip binding vpn-instance** command deletes the IP address of the interface. You must reconfigure the interface's IP address after the association.

Procedures

This example provides only the configurations on the MCE, VR 1, VR 2, VR 3, and PE 1. Configurations on other devices are not shown.

1. Configure VPN instances on the MCE and PE 1:

On the MCE, create a VPN instance named **vpn1**, and configure its RD as 10:1.

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
```

Create a VPN instance named **vpn2**, and configure its RD as 20:1.

```
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
```

Bind VLAN-interface 10 to the VPN instance **vpn1**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 10
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
[MCE-Vlan-interface10] ip address 10.214.10.3 24
```

```
[MCE-Vlan-interface10] quit
```

Bind VLAN-interface 20 to the VPN instance **vpn2**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 20
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
[MCE-Vlan-interface20] ip address 10.214.20.3 24
[MCE-Vlan-interface20] quit
```

Bind VLAN-interface 21 to the VPN instance **vpn2**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 21
[MCE-Vlan-interface21] ip binding vpn-instance vpn2
[MCE-Vlan-interface21] ip address 10.214.50.3 24
[MCE-Vlan-interface21] quit
```

Bind VLAN-interface 30 to the VPN instance **vpn1**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 30
[MCE-Vlan-interface30] ip binding vpn-instance vpn1
[MCE-Vlan-interface30] ip address 172.16.30.1 24
[MCE-Vlan-interface30] quit
```

Bind VLAN-interface 40 to the VPN instance **vpn2**, and configure an IP address for the interface.

```
[MCE] interface Vlan-interface 40
[MCE-Vlan-interface40] ip binding vpn-instance vpn2
[MCE-Vlan-interface40] ip address 172.16.40.1 24
[MCE-Vlan-interface40] quit
```

On PE 1, create VPN instances **vpn1** and **vpn2**, and configure RDs for the VPN instances. Make sure the RDs are the same as those configured on the MCE.

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 10:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 20:1
[PE1-vpn-instance-vpn2] quit
```

Bind VLAN-interface 30 to the VPN instance **vpn1** and VLAN-interface 40 to the VPN instance **vpn2**, and configure IP addresses for the interfaces.

```
[PE1] interface vlan-interface 30
[PE1-Vlan-interface30] ip binding vpn-instance vpn1
[PE1-Vlan-interface30] ip address 172.16.30.2 24
[PE1-Vlan-interface30] quit
[PE1] interface vlan-interface 40
[PE1-Vlan-interface40] ip binding vpn-instance vpn2
[PE1-Vlan-interface40] ip address 172.16.40.2 24
[PE1-Vlan-interface40] quit
```

2. Configure routing between the MCE and VPN sites:

On VR 1, assign IP address 10.214.10.2/24 to the interface connected to the MCE. (Details not shown.)

On VR 1, enable OSPF, and advertise networks 192.168.1.0/24 and 10.214.10.2/24.

```
<VR1> system-view
[VR1] ospf
```

```
[VR1-ospf-1] area 0
[VR1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[VR1-ospf-1-area-0.0.0.0] network 10.214.10.0 0.0.0.255
```

On the MCE, bind Loopback 0 to the VPN instance **vpn1** and configure an IP address for the loopback interface.

```
[MCE] interface LoopBack 0
[MCE-LoopBack0] ip binding vpn-instance vpn1
[MCE-LoopBack0] ip address 101.101.10.1 32
[MCE-LoopBack0] quit
```

On the MCE, enable OSPF process 1, bind the process to the VPN instance **vpn1**, and specify the router ID as the IP address of Loopback 0.

```
[MCE] ospf 1 vpn-instance vpn1 router-id 101.101.10.1
```

On the MCE, advertise the network 10.214.10.0/24.

```
[MCE-ospf-1] area 0
[MCE-ospf-1-area-0.0.0.0] network 10.214.10.0 0.0.0.255
[MCE-ospf-1-area-0.0.0.0] quit
[MCE-ospf-1] quit
```

On the MCE, display the routing table for the VPN instance **vpn1**.

```
[MCE] display ip routing-table vpn-instance vpn1

Destinations : 6        Routes : 6

Destination/Mask   Proto   Pre Cost         NextHop         Interface
0.0.0.0/32         Direct  0   0            127.0.0.1       InLoop0
127.0.0.0/8        Direct  0   0            127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0            127.0.0.1       InLoop0
10.214.10.0/24     Direct  0   0            10.214.10.3     Vlan10
10.214.10.3/32     Direct  0   0            127.0.0.1       InLoop0
192.168.1.0/24     O_INTRA 10  2            10.214.10.2     Vlan10
```

The output shows that the MCE has learned an OSPF route to VPN 1 site 1.

On VR 2, assign IP address 10.214.20.2/24 to the interface connected to the MCE. (Details not shown.)

On VR 3, assign IP address 10.214.50.2/24 to the interface connected to the MCE. (Details not shown.)

On VR 2, enable BGP in AS 100, specify 10.214.20.3 (the MCE) as the peer, and advertise networks 192.168.2.0/24 and 10.214.20.0/24.

```
<VR2> system-view
[VR2] bgp 100
[VR2-bgp-default] router-id 2.2.2.2
[VR2-bgp-default] peer 10.214.20.3 as-number 100
[VR2-bgp-default] address-family ipv4
[VR2-bgp-default-ipv4] peer 10.214.20.3 enable
[VR2-bgp-default-ipv4] network 192.168.2.0 24
[VR2-bgp-default-ipv4] network 10.214.20.0 24
[VR2-bgp-default-ipv4] quit
[VR2-bgp-default] quit
```

On VR 3, enable BGP in AS 100, specify 10.214.50.3 (the MCE) as the peer, and advertise networks 192.168.3.0/24 and 10.214.50.0/24.

```
<VR3> system-view
```

```
[VR3] bgp 100
[VR3-bgp-default] router-id 3.3.3.3
[VR3-bgp-default] peer 10.214.50.3 as-number 100
[VR3-bgp-default] address-family ipv4
[VR3-bgp-default-ipv4] peer 10.214.50.3 enable
[VR3-bgp-default-ipv4] network 192.168.3.0 24
[VR3-bgp-default-ipv4] network 10.214.50.0 24
[VR3-bgp-default-ipv4] quit
[VR3-bgp-default] quit
```

On the MCE, enable BGP in AS 100, create the BGP-VPN instance **vpn2**, specify 10.214.20.2 and 10.214.50.2 as the peers, and advertise networks 10.214.20.0/24 and 10.214.50.0/24.

```
[MCE] bgp 100
[MCE-bgp-default] ip vpn-instance vpn2
[MCE-bgp-default-vpn2] peer 10.214.20.2 as-number 100
[MCE-bgp-default-vpn2] peer 10.214.50.2 as-number 100
[MCE-bgp-default] address-family ipv4
[MCE-bgp-default-ipv4-vpn2] peer 10.214.20.2 enable
[MCE-bgp-default-ipv4-vpn2] peer 10.214.50.2 enable
[MCE-bgp-default-ipv4-vpn2] network 10.214.20.0 24
[MCE-bgp-default-ipv4-vpn2] network 10.214.50.0 24
```

Configure the MCE as a route reflector, and specify VR 2 and VR 3 as its clients.

```
[MCE-bgp-default-ipv4-vpn2] peer 10.214.20.2 reflect-client
[MCE-bgp-default-ipv4-vpn2] peer 10.214.50.2 reflect-client
```

On the MCE, display BGP VPNv4 routing information for the BGP instance **vpn2**.

```
[MCE-bgp-default-ipv4-vpn2] display bgp routing-table vpnv4

BGP local router ID is 4.4.4.4
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 20:1(vpn2)
 Total number of routes: 6

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  10.214.20.0/24     10.214.20.3     0                     32768   i
*  i                    10.214.20.2     0          100        0       i
* >  10.214.50.0/24     10.214.50.3     0                     32768   i
*  i                    10.214.50.2     0          100        0       i
* >i 192.168.2.0        10.214.20.2     0          100        0       i
* >i 192.168.3.0        10.214.50.2     0          100        0       i
```

The output shows that the MCE has learned BGP routes to the sites of VPN 2.

3. Configure routing between the MCE and PE 1:

On the MCE, create the BGP-VPN instance **vpn1**, and specify 172.16.30.2 (PE 1) as the EBGP peer in AS 200.

```
[MCE] bgp 100
[MCE-bgp-default] ip vpn-instance vpn1
[MCE-bgp-default-vpn1] peer 172.16.30.2 as-number 200
```

Redistribute OSPF routes for BGP-VPN instance **vpn1**, and advertise network 172.16.30.0/24.

```
[MCE-bgp-default-vpn1] address-family ipv4
[MCE-bgp-default-ipv4-vpn1] import-route ospf
[MCE-bgp-default-ipv4-vpn1] peer 172.16.30.2 enable
[MCE-bgp-default-ipv4-vpn1] network 172.16.30.0 24
[MCE-bgp-default-ipv4-vpn1] quit
[MCE-bgp-default-vpn1] quit
```

On PE 1, enter the view of the BGP-VPN instance **vpn1**, specify 172.16.30.1 (the MCE) as the EBGP peer in AS 100, and advertise network 172.16.30.0/24.

```
[PE1] bgp 200
[PE1-bgp-default] ip vpn-instance vpn1
[PE1-bgp-default-vpn1] peer 172.16.30.1 as-number 100
[PE1-bgp-default-vpn1] address-family ipv4
[PE1-bgp-default-ipv4-vpn1] peer 172.16.30.1 enable
[PE1-bgp-default-ipv4-vpn1] network 172.16.30.0 24
[PE1-bgp-default-ipv4-vpn1] quit
[PE1-bgp-default-vpn1] quit
```

On the MCE, enter the view of the BGP-VPN instance **vpn2**, specify 172.16.40.2 (PE 1) as the EBGP peer in AS 200, and advertise network 172.16.40.0/24.

```
[MCE-bgp-default] ip vpn-instance vpn2
[MCE-bgp-default-vpn2] peer 172.16.40.2 as-number 200
[MCE-bgp-default-vpn2] address-family ipv4
[MCE-bgp-default-ipv4-vpn2] peer 172.16.40.2 enable
[MCE-bgp-default-ipv4-vpn2] network 172.16.40.0 24
[MCE-bgp-default-ipv4-vpn2] quit
[MCE-bgp-default-vpn2] quit
[MCE-bgp-default] quit
```

On PE 1, enter the view of the BGP-VPN instance **vpn2**, specify 172.16.40.1 (the MCE) as the EBGP peer in AS 100, and advertise network 172.16.40.0/24.

```
[PE1-bgp-default] ip vpn-instance vpn2
[PE1-bgp-default-vpn2] peer 172.16.40.1 as-number 100
[PE1-bgp-default-vpn2] address-family ipv4
[PE1-bgp-default-ipv4-vpn2] peer 172.16.40.1 enable
[PE1-bgp-default-ipv4-vpn2] network 172.16.40.0 24
[PE1-bgp-default-ipv4-vpn2] quit
[PE1-bgp-default-vpn2] quit
[PE1-bgp-default] quit
```

Verifying the configuration

On PE 1, verify that the VPN instance **vpn1** has learned the BGP route to VPN 1 site 1.

```
[PE1] display ip routing-table vpn-instance vpn1

Destinations : 5        Routes : 5
```

```
Destination/Mask    Proto  Pre  Cost        NextHop         Interface

127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
172.16.30.0/24      Direct 0    0           172.16.30.2     Vlan30
172.16.30.2/24      Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      BGP    255  3           172.16.30.1     Vlan30
```

On PE 1, verify that the VPN instance **vpn2** has learned the BGP routes to the sites of VPN 2.

```
[PE1] display ip routing-table vpn-instance vpn2

Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.214.20.0/24      BGP     255 0           172.16.40.1     Vlan40
10.214.50.0/24      BGP     255 0           172.16.40.1     Vlan40
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.40.0/24      Direct  0   0           172.16.40.2     Vlan40
172.16.40.0/32      Direct  0   0           172.16.40.2     Vlan40
172.16.40.2/32      Direct  0   0           127.0.0.1       InLoop0
172.16.40.255/32    Direct  0   0           172.16.40.2     Vlan40
192.168.2.0/24      BGP     255 0           172.16.40.1     Vlan40
192.168.3.0/24      BGP     255 0           172.16.40.1     Vlan40
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- VR 1:

```
#
ospf 1
 area 0.0.0.0
  network 10.214.10.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
 vlan 10
#
interface Vlan-interface10
 ip address 10.214.10.2 255.255.255.0
#
```

- VR 2:

```
#
 vlan 20
#
interface Vlan-interface20
 ip address 10.214.20.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.214.20.3 as-number 100
 #
 address-family ipv4 unicast
  network 10.214.20.0 255.255.255.0
  network 192.168.2.0 255.255.255.0
  peer 10.214.20.3 enable
#
```

- VR 3:

```
#
 vlan 21
#
interface Vlan-interface21
 ip address 10.214.50.2 255.255.255.0
#
bgp 100
 router-id 3.3.3.3
 peer 10.214.50.3 as-number 100
 #
 address-family ipv4 unicast
  network 3.3.3.3 255.255.255.255
  network 10.214.50.0 255.255.255.0
  network 192.168.3.0 255.255.255.0
  peer 10.214.50.3 enable
#
```

- MCE:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
vlan 10
#
vlan 20 to 21
#
vlan 30
#
vlan 40
```

```
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 101.101.10.1 255.255.255.255
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface21
 ip binding vpn-instance vpn2
 ip address 10.214.50.3 255.255.255.0
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.1 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.1 255.255.255.0
#
bgp 100
 #
 address-family ipv4 unicast
 #
 ip vpn-instance vpn1
  peer 172.16.30.2 as-number 200
  #
  address-family ipv4 unicast
   import-route ospf 1
   network 172.16.30.0 255.255.255.0
 #
 ip vpn-instance vpn2
  peer 10.214.20.2 as-number 100
  peer 10.214.50.2 as-number 100
  peer 172.16.40.2 as-number 200
  #
  address-family ipv4 unicast
   network 10.214.20.0 255.255.255.0
   network 10.214.50.0 255.255.255.0
   network 172.16.40.0 255.255.255.0
   peer 10.214.20.2 enable
   peer 10.214.20.2 reflect-client
   peer 10.214.50.2 enable
```

```
   peer 10.214.50.2 reflect-client
   peer 172.16.40.2 enable
#
ospf 1 router-id 101.101.10.1 vpn-instance vpn1
 area 0.0.0.0
  network 10.214.10.0 0.0.0.255
#
```

- PE 1:

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip binding vpn-instance vpn1
 ip address 100.100.11.1 255.255.255.255
#
interface LoopBack1
 ip binding vpn-instance vpn2
 ip address 100.100.21.1 255.255.255.255
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.2 255.255.255.0
#
interface Vlan-interface40
 ip binding vpn-instance vpn2
 ip address 172.16.40.2 255.255.255.0
#
bgp 200
 #
 ip vpn-instance vpn1
  peer 172.16.30.1 as-number 100
  #
  address-family ipv4 unicast
   network 172.16.30.0 255.255.255.0
   peer 172.16.30.1 enable
 #
 ip vpn-instance vpn2
  peer 172.16.40.1 as-number 100
  #
  address-family ipv4 unicast
```

```
    network 172.16.40.0 255.255.255.0
    peer 172.16.40.1 enable
#
```

Contents

Introduction

This document provides configuration examples of link layer attack protection, ARP attack protection, network layer attack protection, and transport layer attack protection, as defined in Table 1.

Table 1 Attack protection types

Attack protection types		Description
Link layer attack protection	MAC address attack protection	Prevents the attack of packets with different source MAC addresses or VLANs by configuring the maximum number of MAC addresses that an interface can learn.
	STP packet attack protection	Provides protection measures such as BPDU guard, root guard, loop guard, and TC-BPDU guard.
ARP attack protection	ARP source suppression	Prevents IP attack packets from fixed sources.
	ARP black hole routing	Prevents IP attack packets from sources that are not fixed.
	ARP active acknowledgement	Prevents user spoofing.
	Source MAC-based ARP attack detection	Prevents ARP packet attacks from the same source MAC.
	ARP packet source MAC consistency check	Prevents attacks from ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.
Network layer attack protection	uRPF check	Protects a network against source spoofing attacks.
	TTL attack protection	Prevents an attack by disabling sending ICMP time exceeded messages.
Transport layer attack protection	SYN flood attack protection	Enables the server to return a SYN ACK message when it receives a TCP connection request, without establishing a half-open TCP connection.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of attack protection.

Example: Configuring link layer attack protection

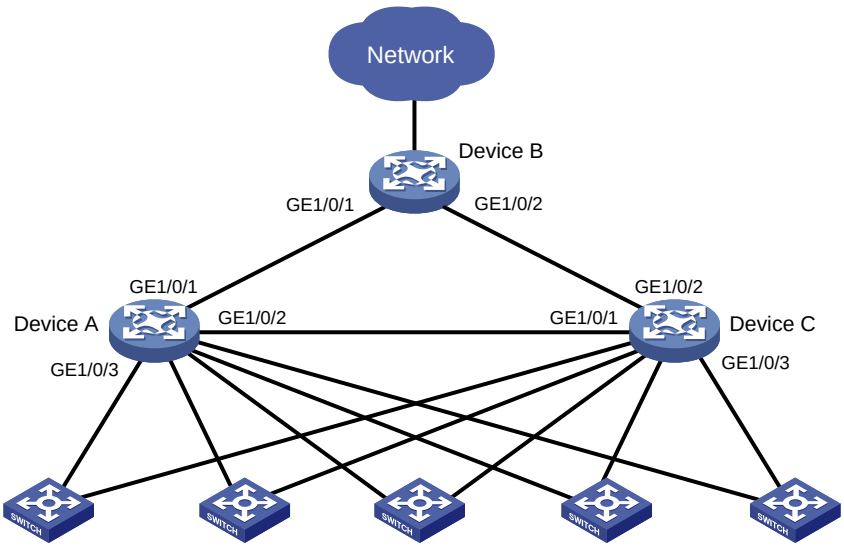
Network configuration

As shown in Figure 1, Device A, Device B, and Device C run MSTP. Device B acts as the root bridge, and GigabitEthernet 1/0/1 on Device C is blocked.

Configure the following features to prevent link layer attacks:

- Configure root guard on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Device B for Device B to act as the root bridge.
- Configure loop guard on GigabitEthernet 1/0/2 of Device C to prevent temporary loops. The loop guard feature keeps the port in **Discarding** state in all MSTIs when it receives no BPDU.
- Configure BPDU guard on ports at the access side of Device A and Device C. The BPDU guard feature prevents the ports from performing spanning tree calculations when it receives forged BPDUs with a higher priority.
- Enable TC-BPDU guard on Device A, Device B, and Device C. The TC-BPDU guard feature prevents a large number of TC-BPDUs from affecting the network in a short time.
- Set the maximum number of MAC addresses that can be learned by ports at the access side of Device A and Device C. This configuration protects the devices from a large number of attack packets that have different source MAC addresses. The attack packets might cause a large MAC table and low forwarding performance.
- Configure broadcast and multicast suppression on the designated ports of Device B and all ports on Device A and Device C. When incoming broadcast or multicast traffic exceeds the threshold (6400 pps), an interface discards broadcast or multicast packets until the traffic drops below the threshold.

Figure 1 Network diagram



Analysis

For the ports at the access side of Device A and Device C to rapidly transit to the forwarding state, use the **stp edged-port** command to configure these ports as edge ports.

This example uses GigabitEthernet 1/0/3 to illustrate the configuration on the ports at the access side on Device A and Device C.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch	Release 63xx

Hardware	Software version
S5500V3-48P-SI switch	
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx

Hardware	Software version
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 63xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure link layer attack protection, follow these restrictions and guidelines:

- On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.
- Do not configure the loop guard feature on ports at the access side. Otherwise, the ports stay in **Discarding** state in all MSTIs because they cannot receive BPDUs.

Procedures

Configuring Device B

Specify IP addresses for interfaces. (Details not shown.)

Configure root guard on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceB> system-view
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceB-if-range] stp root-protection
[DeviceB-if-range] quit
```

Configure TC-BPDU guard.

```
[DeviceB] stp tc-protection
[DeviceB] stp tc-protection threshold 10
```

Configure broadcast and multicast suppression on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceB-if-range] broadcast-suppression pps 6400
[DeviceB-if-range] multicast-suppression pps 6400
[DeviceB-if-range] quit
```

Configuring Device A

Specify IP addresses for interfaces. (Details not shown.)

Configure STP BPDU guard.

```
<DeviceA> system-view
[DeviceA] stp bpdu-protection
```

Configure GigabitEthernet 1/0/3 as an edge port.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] stp edged-port
```

```
[DeviceA-GigabitEthernet1/0/3] quit
```

Configure TC-BPDU guard.

```
[DeviceA] stp tc-protection
[DeviceA] stp tc-protection threshold 10
```

Set the maximum number of MAC addresses that GigabitEthernet 1/0/3 can learn.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] mac-address max-mac-count 1024
[DeviceA-GigabitEthernet1/0/3] quit
```

Configure broadcast and multicast suppression on all ports.

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] broadcast-suppression pps 6400
[DeviceA-if-range] multicast-suppression pps 6400
[DeviceA-if-range] quit
```

Configuring Device C

Specify IP addresses for interfaces. (Details not shown.)

Configure STP BPDU guard.

```
<DeviceC> system-view
[DeviceC] stp bpdu-protection
```

Configure GigabitEthernet 1/0/3 as an edge port.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] stp edged-port
[DeviceC-GigabitEthernet1/0/3] quit
```

Configure loop guard on GigabitEthernet 1/0/2.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] stp loop-protection
[DeviceC-GigabitEthernet1/0/2] quit
```

Configure TC-BPDU guard.

```
[DeviceC] stp tc-protection
[DeviceC] stp tc-protection threshold 10
```

Set the maximum number of MAC addresses that GigabitEthernet 1/0/3 can learn.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] mac-address max-mac-count 1024
[DeviceC-GigabitEthernet1/0/3] quit
```

Configure broadcast and multicast suppression on all ports.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceC-if-range] broadcast-suppression pps 6400
[DeviceC-if-range] multicast-suppression pps 6400
[DeviceC-if-range] quit
```

Verifying the configuration

Verify that the edge ports go down after they receives STP BPDUs. (Details not shown.)

Bring the edge ports up by using the **undo shutdown** command. (Details not shown.)

Verify that the bridge ID of Device B does not change and that the STP topology remains stable after STP BPDUs with higher priority are sent to Device B. (Details not shown.)

Verify that the devices do not refresh the FIB table frequently and that no serious packet loss occurs after a large number of TC BPDUs are sent to the devices. (Details not shown.)

Verify that the uplink ports are not flooded after a large number of broadcasts are sent to the edge ports on device A and Device C. (Details not shown.)

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
stp bpdu-protection
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
 port link-mode bridge
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
 port link-mode bridge
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/3
 port link-mode bridge
 mac-address max-mac-count 1024
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
```

- Device B:

```
#
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
 port link-mode bridge
 stp root-protection
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
 port link-mode bridge
 stp root-protection
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
```

```
#
```

- Device C:

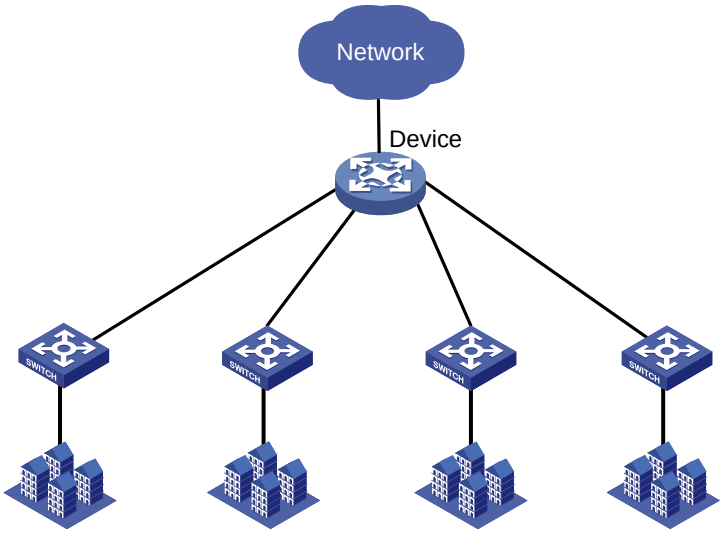
```
#
stp bpdu-protection
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
 port link-mode bridge
 stp root-protection
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
 port link-mode bridge
 stp loop-protection
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/3
 port link-mode bridge
 stp edged-port
 mac-address max-mac-count 1024
 broadcast-suppression pps 6400
 multicast-suppression pps 6400
#
```

Example: Configuring ARP attack protection

Network configuration

As shown in Figure 2, the device is the gateway for the internal network. Configure ARP attack protection on the device to prevent ARP attacks.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6628Pxx

Hardware	Software version
ES5500 switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx

Hardware	Software version
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 63xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Specify IP addresses for interfaces. (Details not shown.)

Enable ARP source suppression.

```
<Device> system-view
[Device] arp source-suppression enable
```

Configure the device to accept a maximum of 8 unresolvable packets per source IP address in 5 seconds.

```
[Device] arp source-suppression limit 8
```

Enable ARP black hole routing to prevent unresolvable IP packet attacks.

```
[Device] arp resolving-route enable
```

Enable ARP active acknowledgment to prevent user spoofing.

```
[Device] arp active-ack enable
```

Configure source MAC-based ARP attack detection to prevent ARP packet attacks from the same source MAC.

NOTE:

The IE4520 switch series does support the source MAC-based ARP attack detection feature.

```
[Device] arp source-mac filter
[Device] arp source-mac threshold 25
```

Enable ARP packet source MAC address consistency check to prevent attacks from ARP packets with different source MAC addresses in the Ethernet header and in the message body.

```
[Device] arp valid-check enable
```

Verifying the configuration

1. Verify that ARP attack protection functions on the device:

   # Send ARP attack packets to the device. (Details not shown.)

   # Verify that the CPU usage does not surge. (Details not shown.)
2. Verify that each ARP attack protection feature functions on the device (this example uses the ARP source suppression feature):

Send the device 20 forged packets with the same source IP address and unresolvable destination IP addresses. (Details not shown.)

Verify that the device stops resolving the packets after receiving 8 forged packets within 5 seconds. (Details not shown.)

Verify the ARP source suppression configuration.

```
[Device] display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 8
 Current cache length: 16
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 arp valid-check enable
 arp source-mac filter
 arp source-mac threshold 25
 arp active-ack enable
 arp source-suppression enable
 arp source-suppression limit 8
#
```

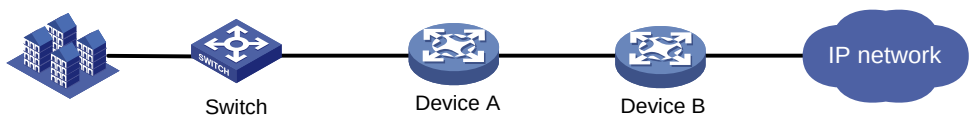
Example: Configuring network layer attack protection

Network configuration

As shown in Figure 3, Device A is the gateway for the internal network. To protect Device A against IP packet attacks from internal and external networks, configure the following network layer attack protection features:

- Configure strict uRPF check to prevent source address spoofing attacks.
- Disabling sending ICMP time exceeded messages. The device will not be flooded by ICMP time exceeded messages when receiving a large number of packets with TTL set to 1.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 63xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure network layer attack protection, follow these restrictions and guidelines:

- After you disable sending ICMP time exceeded messages, the tracert feature will not be available.
- Enabling the uRPF check feature halves the route capacity of the switch.
- The uRPF check feature cannot be enabled if the number of existing routes exceeds half of the route capacity on the switch. This mechanism prevents route loss, which can cause packet loss.

Procedures

Specify IP addresses for interfaces. (Details not shown.)

Enable strict uRPF check.

```
[DeviceA] ip urpf strict
```

Disable sending ICMP time exceeded messages. Sending ICMP time exceeded messages is disabled by default.

```
[DeviceA] undo ip ttl-expires enable
```

Verifying the configuration

1. Verify that Device A can prevent source address spoofing attacks:

   # Verify that Device A can filter out packets with forged source IP addresses. (Details not shown.)

   # Verify the uRPF configuration.

   ```
   [DeviceA] display ip urpf
   Global uRPF configuration information:
      Check type: strict
   ```

2. Verify that TTL attack protection functions on Device A:

   # Enable ICMP debugging by executing the **`debugging ip icmp`** command on Device A. (Details not shown.)

   # Use a PC to send packets in which the TTL is 1 to Device A. (Details not shown.)

   # Verify that Device A does not display any debugging information and that the PC does not receive any ICMP time exceeded messages. (Details not shown.)

   # Enable sending ICMP time exceeded messages and send packets in which the TTL is 1 to Device A. (Details not shown.)

   # Verify that Device A responds with ICMP time exceeded messages.

   ```
   <DeviceA> *Aug 14 16:43:31:068 2016 NM-3 SOCKET/7/ICMP: Slot=2;
   Time(s):1371221011  ICMP Output:
    ICMP Packet: src = 6.0.0.1, dst = 202.101.0.2
                 type = 11, code = 0 (ttl-exceeded)
    Original IP: src = 202.101.0.2, dst = 192.168.0.2
                 proto = 253, first 8 bytes = 00000000 00000000
   ```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

#

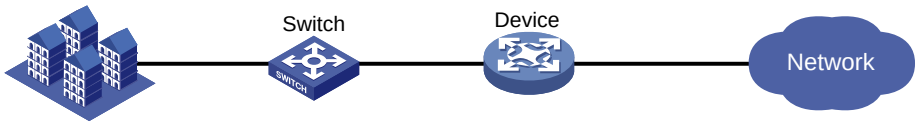
```
ip urpf strict
#
```

Example: Configuring transport layer attack protection

Network configuration

As shown in Figure 4, the device is the gateway for the internal network. Configure SYN Cookie protection on the device to protect against SYN flood attacks. With this feature enabled, the device responds to a SYN packet with a SYN ACK packet without establishing a TCP semi-connection. The device establishes a TCP connection only when it receives an ACK packet from the sender.

Figure 4 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6628Pxx

Hardware	Software version
S5000-EI switch series	Release 63xx, Release 65xx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 63xx
S5135S-EI switch series	Release 6658P01 and later

Procedures

Specify IP addresses for interfaces. (Details not shown.)

Enable SYN Cookie.

```
<Device> system-view
[Device] tcp syn-cookie enable
```

Verifying the configuration

Verify that the device does not have any TCP semi-connections. The state "SYN_RECEIVED" represents semi-connections.

```
[Device] display tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Slot  PCB
 0.0.0.0:21            0.0.0.0:0             LISTEN      1     0xfffffffffffff9
d
 0.0.0.0:23            0.0.0.0:0             LISTEN      1     0xfffffffffffff9
f
 192.168.2.88:23       192.168.2.79:2197     ESTABLISHED 1     0xfffffffffffffa
3
 192.168.2.88:23       192.168.2.89:2710     ESTABLISHED 1     0xfffffffffffffa
2
 192.168.2.88:23       192.168.2.110:50199   ESTABLISHED 1     0xfffffffffffffa
5
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
   tcp syn-cookie enable
#
```

Contents

Introduction

This document provides Smart Link configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of Smart Link, Monitor Link, and IRF.

General restrictions and guidelines

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group configuration takes effect. The port is not shown in the output from the **`display smart-link group`** command.

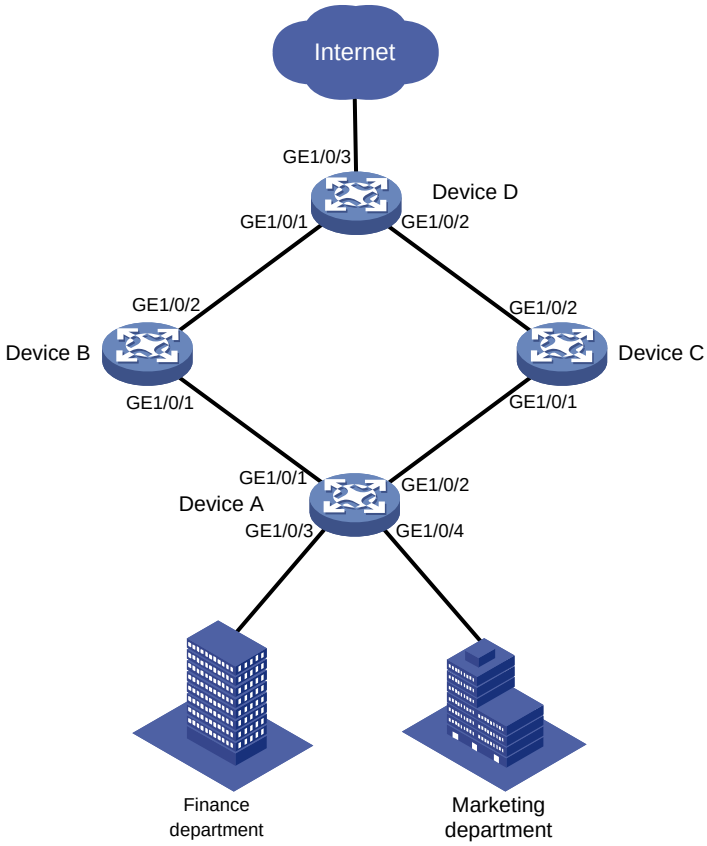
Example: Configuring Smart Link load sharing

Network configuration

As shown in Figure 1, VLAN 10 and VLAN 11 are assigned to the Finance department and the Marketing department of an enterprise, respectively. Traffic of VLAN 10 and VLAN 11 on Device A is dually uplinked to Device D by Device B and Device C. Configure Smart Link to meet the following requirements:

- When the link between Device A and Device B and the link between Device A and Device C are both available, the traffic of the Finance department is forwarded trough the link between Device A and Device B. The traffic of the Marketing department is forwarded through the link between Device A and Device C.
- When one link fails, the traffic on the link is switched to another link. When the link recovers, the traffic is switched back to the link.

Figure 1 Network diagram



Device	Interface	VLAN	Device	Interface	VLAN
Device A	GE1/0/1	10, 11	Device C	GE1/0/1	10, 11
	GE1/0/2	10, 11		GE1/0/2	10, 11
	GE1/0/3	10	Device D	GE1/0/1	10, 11
	GE1/0/4	11		GE1/0/2	10, 11
Device B	GE1/0/1	10, 11		GE1/0/3	10, 11
	GE1/0/2	10, 11			

Analysis

To implement load sharing on the two uplinks, create two smart link groups with the same member ports on Device A. The role of each port must be different in the two smart link groups. Use the VLANs of the Finance department and Marketing department as the protected VLANs of the corresponding smart link groups.

For the traffic to switch back to the recovered link, enable role preemption for the two smart link groups.

For the upstream device to refresh MAC address entries and ARP/ND entries when link switchover occurs in a smart link group, perform the following tasks:

- Enable flush message sending on Device A.
- Enable flush message receiving on ports of the primary and secondary links from Device A to Device D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure Smart Link load sharing, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Before you configure a smart link group member port or its directly connected port, disable the spanning tree feature and RRPP on the port.
- Make sure the receive control VLAN configured on the upstream device is the same as the transmit control VLAN configured on the smart link device.
- The control VLAN configured for a smart link group must be different from the control VLAN configured for any other smart link groups.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

Procedures

Configuring Device A

1. Create VLAN 10 and VLAN 11.

```
<DeviceA> system-view
[DeviceA] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Shut down GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 10 11
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as an access port and assign the port to VLAN 10.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 10
```

Bring up the port.

```
[DeviceA-GigabitEthernet1/0/3] undo shutdown
[DeviceA-GigabitEthernet1/0/3] quit
```

5. Configure GigabitEthernet 1/0/4:

Configure GigabitEthernet 1/0/4 as an access port and assign the port to VLAN 11.

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port access vlan 11
```

Bring up the port.

```
[DeviceA-GigabitEthernet1/0/4] undo shutdown
[DeviceA-GigabitEthernet1/0/4] quit
```

6. Configure VLAN-to-MSTI mappings and activate the MST region configuration:

Enter MST region view.

```
[DeviceA] stp region-configuration
```

Map VLAN 10 to MSTI 1, and VLAN 11 to MSTI 2.

```
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 11
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

7. Configure smart link group 1:

Create smart link group 1 and configure the VLAN mapped to MSTI 1, VLAN 10, as the protected VLAN.

```
[DeviceA] smart-link group 1
[DeviceA-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceA-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Enable flush message sending, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceA-smlk-group1] flush enable control-vlan 10
```

Enable role preemption and set the preemption delay to 10 seconds.

```
[DeviceA-smlk-group1] preemption mode role
[DeviceA-smlk-group1] preemption delay 10
[DeviceA-smlk-group1] quit
```

8. Configure smart link group 2:

Create smart link group 2 and configure the VLAN mapped to MSTI 2, VLAN 11, as the protected VLAN.

```
[DeviceA] smart-link group 2
[DeviceA-smlk-group2] protected-vlan reference-instance 2
```

Configure GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port.

```
[DeviceA-smlk-group2] port gigabitethernet 1/0/2 primary
[DeviceA-smlk-group2] port gigabitethernet 1/0/1 secondary
```

Enable flush message sending, and configure VLAN 11 as the transmit control VLAN.

```
[DeviceA-smlk-group2] flush enable control-vlan 11
```

Enable role preemption and set the preemption delay to 10 seconds.

```
[DeviceA-smlk-group2] preemption mode role
```

```
[DeviceA-smlk-group2] preemption delay 10
[DeviceA-smlk-group2] quit
```

9. Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B

1. Create VLAN 10 and VLAN 11.

```
<DeviceB> system-view
[DeviceB] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceB-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceB-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

1. Create VLAN 10 and VLAN 11.

```
<DeviceC> system-view
[DeviceC] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceC-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceC-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLAN 10 and VLAN 11.

```
<DeviceD> system-view
[DeviceD] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 10 11
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as a trunk port

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Bring up the port.

```
[DeviceD-GigabitEthernet1/0/3] undo shutdown
[DeviceD-GigabitEthernet1/0/3] quit
```

Verifying the configuration

1. Verify the smart link group configuration when Device A is operating correctly:

Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  0               NA
  GE1/0/2                 SECONDARY STANDBY 2               16:22:40 2019/10/29

Smart link group 2 information:
  Device ID       : 0000-fc00-2500
```

```
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 11
  Protected VLAN  : Reference Instance 2

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/2                 PRIMARY   ACTIVE  2               16:22:40 2019/10/29
  GE1/0/1                 SECONDARY STANDBY 0               NA
```

The output shows the following information:

- In smart link group 1, the primary port GigabitEthernet 1/0/1 is active to transmit traffic from VLAN 10.
- In smart link group 2, the primary port GigabitEthernet 1/0/2 is active to transmit traffic from VLAN 11.

2. Verify the smart link group configuration when GigabitEthernet 1/0/1 on Device A is down:

Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   DOWN    0               NA
  GE1/0/2                 SECONDARY ACTIVE  3               16:43:06 2019/10/29

Smart link group 2 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 11
  Protected VLAN  : Reference Instance 2

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/2                 PRIMARY   ACTIVE  2               16:22:40 2019/10/29
  GE1/0/1                 SECONDARY DOWN    0               NA
```

The output shows the following information:

- In smart link group 1, the secondary port GigabitEthernet 1/0/2 is active to transmit traffic from VLAN 10.
- In smart link group 2, the primary port GigabitEthernet 1/0/2 remains active to transmit traffic from VLAN 11.

Display information about the received flush messages on Device B.

```
[DeviceB] display smart-link flush
 Received flush packets                      : 1
```

```
 Receiving interface of the last flush packet : GigabitEthernet1/0/2
 Receiving time of the last flush packet      : 16:43:08 2019/10/29
 Device ID of the last flush packet           : 0000-fc00-2500
 Control VLAN of the last flush packet        : 10
```

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 1
#
vlan 10 to 11
#
stp region-configuration
 instance 1 vlan 10
 instance 2 vlan 11
 active region-configuration
#
smart-link group 1
 preemption mode role
 preemption delay 10
 flush enable control-vlan 10
 protected-vlan reference-instance 1
#
smart-link group 2
 preemption mode role
 preemption delay 10
 flush enable control-vlan 11
 protected-vlan reference-instance 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 port smart-link group 1 primary
 port smart-link group 2 secondary
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
```

```
 port smart-link group 1 secondary
 port smart-link group 2 primary
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 11
#
```

- Device B:

```
#
vlan 1
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
```

- Device C:

```
#
vlan 1
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
```

- Device D:

```
#
vlan 1
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
#
```

Example: Configuring Smart Link and Monitor Link collaboration

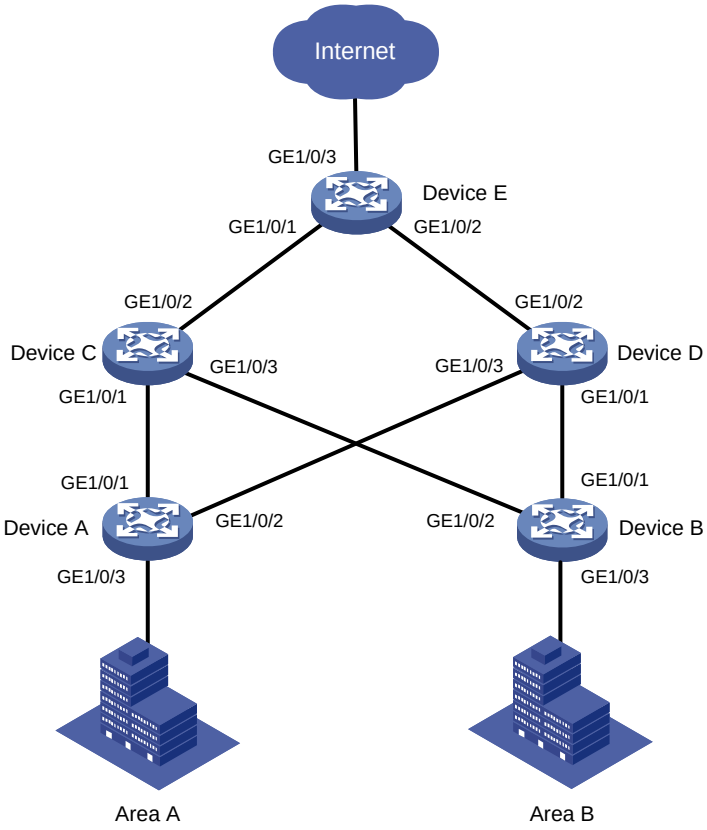
Network configuration

As shown in Figure 2, VLAN 10 and VLAN 11 are assigned to Zone A and Zone B, respectively. Traffic of VLAN 10 is dually uplinked from Device A to Device E by Device C and Device D. Traffic of VLAN 11 is dually uplinked from Device B to Device E by Device C and Device D. Configure Smart Link and Monitor Link to meet the following requirements:

- When the link between Device A and Device C and the link between Device A and Device D are both available, the traffic of Zone A is forwarded trough the link between Device A and Device C. When the link between Device A and Device C fails, the traffic is switched to the link between Device A and Device D. When the link between Device A and Device C recovers, the traffic switches back to the link.

- When the link between Device B and Device C and the link between Device B and Device D are both available, the traffic of Zone B is forwarded trough the link between Device B and Device D. When the link between Device B and Device D fails, the traffic is switched to the link between Device B and Device C. When the link between Device B and Device D recovers, the traffic switches back to the link.
- Configure Monitor Link on Device C and Device D to associate the state of downlink interfaces with the state of uplink interfaces. When Monitor link shuts down the downlink interfaces because of an uplink failure, Smart Link triggers a link switchover.

Figure 2 Network diagram



Device	Interface	VLAN	Device	Interface	VLAN
Device A	GE1/0/1	10	Device D	GE1/0/1	11
	GE1/0/2	10		GE1/0/2	10, 11
	GE1/0/3	10		GE1/0/3	10
Device B	GE1/0/1	11	Device E	GE1/0/1	10, 11
	GE1/0/2	11		GE1/0/2	10, 11
	GE1/0/3	11		GE1/0/3	10, 11
Device C	GE1/0/1	10			
	GE1/0/2	10, 11			
	GE1/0/3	11			

Analysis

To implement dual uplink backup on Device A and Device B, perform the following tasks:

- Create a smart link group on Device A and Device B, respectively.

- Configure the VLANs of Zone A and Zone B as the protected VLANs of the corresponding smart link groups.

For the traffic to switch back to the recovered link, enable role preemption for the two smart link groups.

For the upstream device to refresh MAC address forwarding entries and ARP/ND entries when link switchover occurs in a smart link group, perform the following tasks:

- Enable flush message sending on Device A and Device B.
- Enable flush message receiving on the downlink ports on Device C and Device D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx

S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported

IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure Smart Link and Monitor Link collaboration, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Before you configure a smart link group member port or its directly connected port, disable the spanning tree feature and RRPP on the port.
- Make sure the receive control VLAN configured on the upstream device is the same as the transmit control VLAN configured on the smart link device.
- The control VLAN configured for a smart link group must be different from the control VLAN configured for any other smart link groups.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- You can assign a port to only one monitor link group.
- Do not use the **shutdown** command or the **undo shutdown** command to change the state of the downlink interfaces in a monitor link group.

Procedures

Configuring Device A

1. Create VLAN 10 and VLAN 11.

```
<DeviceA> system-view
[DeviceA] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Shut down GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10
```

Remove the port from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 10
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as an access port and assign the port to VLAN 10.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 10
```

Bring up the port.

```
[DeviceA-GigabitEthernet1/0/3] undo shutdown
[DeviceA-GigabitEthernet1/0/3] quit
```

5. Configure VLAN-to-MSTI mappings and activate the MST region configuration:

Enter MST region view.

```
[DeviceA] stp region-configuration
```

Map VLAN 10 to MSTI 1.

```
[DeviceA-mst-region] instance 1 vlan 10
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

6. Configure smart link group 1:

Create smart link group 1 and configure the VLAN mapped to MSTI 1, VLAN 10, as the protected VLAN.

```
[DeviceA] smart-link group 1
[DeviceA-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceA-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceA-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Enable flush message sending, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceA-smlk-group1] flush enable control-vlan 10
```

Enable role preemption and set the preemption delay to 10 seconds.

```
[DeviceA-smlk-group1] preemption mode role
[DeviceA-smlk-group1] preemption delay 10
[DeviceA-smlk-group1] quit
```

7. Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B

1. Create VLAN 10 and VLAN 11.

```
<DeviceB> system-view
[DeviceB] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Shut down GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] shutdown
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 11.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 11
```

Remove the port from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] shutdown
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 11
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as an access port and assign the port to VLAN 11.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port access vlan 11
```

Bring up the port.

```
[DeviceB-GigabitEthernet1/0/3] undo shutdown
[DeviceB-GigabitEthernet1/0/3] quit
```

5. Configure VLAN-to-MSTI mappings and activate the MST region configuration:

Enter MST region view.

```
[DeviceB] stp region-configuration
```

Map VLAN 11 to MSTI 1.

```
[DeviceB-mst-region] instance 1 vlan 11
```

Activate the MST region configuration

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

6. Configure smart link group 1.

Create smart link group 1 and configure the VLAN mapped to MSTI 1, VLAN 11, as the protected VLAN.

```
[DeviceB] smart-link group 1
[DeviceB-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
[DeviceB-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceB-smlk-group1] port gigabitethernet 1/0/2 secondary
```

Enable flush message sending, and configure VLAN 11 as the transmit control VLAN.

```
[DeviceA-smlk-group1] flush enable control-vlan 11
```

Enable role preemption and set the preemption delay to 10 seconds.

```
[DeviceB-smlk-group1] preemption mode role
[DeviceB-smlk-group1] preemption delay 10
[DeviceB-smlk-group1] quit
```

7. Bring up GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2:

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

1. Create VLAN 10 and VLAN 11.

```
<DeviceC> system-view
[DeviceC] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 10
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Enable flush message receiving and configure VLAN 10 as the receive control VLAN on the port.

```
[DeviceC-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10
```

Bring up the port.

```
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceC-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLAN 11.

```
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 11
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
```

Enable flush message receiving and configure VLAN 11 as the receive control VLAN on the port.

```
[DeviceC-GigabitEthernet1/0/3] smart-link flush enable control-vlan 11
```

Bring up the port.

```
[DeviceB-GigabitEthernet1/0/3] undo shutdown
[DeviceB-GigabitEthernet1/0/3] quit
```

5. Configure monitor link group 1:

Create monitor link group 1.

```
[DeviceC] monitor-link group 1
```

Configure the uplink interface threshold for triggering monitor link group state switchover as 1.

```
[DeviceC-mtlk-group1] uplink up-port-threshold 1
```

Configure GigabitEthernet 1/0/2 as the uplink port and GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 as the downlink ports.

```
[DeviceC-mtlk-group1] port gigabitethernet 1/0/2 uplink
[DeviceC-mtlk-group1] port gigabitethernet 1/0/1 downlink
[DeviceC-mtlk-group1] port gigabitethernet 1/0/3 downlink
[DeviceC-mtlk-group1] quit
```

Configuring Device D

1. Create VLAN 10 and VLAN 11.

```
<DeviceD> system-view
[DeviceD] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 11.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 11
```

Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

Enable flush message receiving and configure VLAN 11 as the receive control VLAN on the port.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 11
```

Bring up the port.

```
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
```

Assign the port to VLAN 10.

```
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 10
```

Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/3] undo stp enable
```

Enable flush message receiving and configure VLAN 10 as the receive control VLAN on the port.

```
[DeviceD-GigabitEthernet1/0/3] smart-link flush enable control-vlan 10
```

Bring up the port.

```
[DeviceD-GigabitEthernet1/0/3] undo shutdown
[DeviceD-GigabitEthernet1/0/3] quit
```

5. Configure monitor link group 1:

Create monitor link group 1.

```
[DeviceD] monitor-link group 1
```

Configure the uplink interface threshold for triggering monitor link group state switchover as 1.

```
[DeviceD-mtlk-group1] uplink up-port-threshold 1
```

Configure GigabitEthernet 1/0/2 as the uplink port and GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 as the downlink ports.

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/2 uplink
[DeviceD-mtlk-group1] port gigabitethernet 1/0/1 downlink
```

```
[DeviceD-mtlk-group1] port gigabitethernet 1/0/3 downlink
[DeviceD-mtlk-group1] quit
```

Configuring Device E

1. Create VLAN 10 and VLAN 11.

   ```
   <DeviceE> system-view
   [DeviceE] vlan 10 to 11
   ```

2. Configure GigabitEthernet 1/0/1:

   # Configure GigabitEthernet 1/0/1 as a trunk port.

   ```
   [DeviceE] interface gigabitethernet 1/0/1
   [DeviceE-GigabitEthernet1/0/1] port link-type trunk
   ```

   # Assign the port to VLAN 10 and VLAN 11.

   ```
   [DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 10 11
   ```

   # Remove the port from VLAN 1.

   ```
   [DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
   ```

   # Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

   ```
   [DeviceE-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
   ```

   # Bring up the port.

   ```
   [DeviceE-GigabitEthernet1/0/1] undo shutdown
   [DeviceE-GigabitEthernet1/0/1] quit
   ```

3. Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

   ```
   [DeviceE] interface gigabitethernet 1/0/2
   [DeviceE-GigabitEthernet1/0/2] port link-type trunk
   [DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 10 11
   [DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
   [DeviceE-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
   [DeviceE-GigabitEthernet1/0/2] undo shutdown
   [DeviceE-GigabitEthernet1/0/2] quit
   ```

4. Configure GigabitEthernet 1/0/3:

   # Configure GigabitEthernet 1/0/3 as a trunk port.

   ```
   [DeviceE] interface gigabitethernet 1/0/3
   [DeviceE-GigabitEthernet1/0/3] port link-type trunk
   ```

   # Assign the port to VLAN 10 and VLAN 11.

   ```
   [DeviceE-GigabitEthernet1/0/3] port trunk permit vlan 10 11
   ```

   # Remove the port from VLAN 1.

   ```
   [DeviceE-GigabitEthernet1/0/3] undo port trunk permit vlan 1
   ```

   # Bring up the port.

   ```
   [DeviceE-GigabitEthernet1/0/3] undo shutdown
   [DeviceE-GigabitEthernet1/0/3] quit
   ```

Verifying the configuration

1. Verify the smart link group configuration when Device A and Device B are operating correctly:

   # Display information about all smart link groups on Device A.

   ```
   [DeviceA] display smart-link group all
   ```

```
Smart link group 1 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  1               17:37:49 2019/10/29
  GE1/0/2                 SECONDARY STANDBY 3               17:43:06 2019/10/29
```

The output shows that in smart link group 1, the primary port GigabitEthernet 1/0/1 is active to transmit traffic from VLAN 10.

Display information about all smart link groups on Device B.

```
[DeviceB] display smart-link group all
Smart link group 1 information:
  Device ID       : 0000-fc01-2501
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 11
  Protected VLAN  : Reference Instance 2

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  2               17:22:40 2019/10/29
  GE1/0/2                 SECONDARY STANDBY 0               NA
```

The output shows that in smart link group 1, the primary port GigabitEthernet 1/0/1 is active to transmit traffic from VLAN 11.

2. Verify the monitor link group configuration when Device C and Device D are operating correctly:

Display information about all monitor link groups on Device C.

```
[DeviceC] display monitor-link group all
Monitor link group 1 information:
  Group status     : UP
  Downlink up-delay: 0(s)
  Last-up-time     : 17:07:26 2019/10/29
  Last-down-time   : -
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------
  GE1/0/2                   UPLINK     UP
  GE1/0/1                   DOWNLINK   UP
  GE1/0/3                   DOWNLINK   UP
```

The output shows that in monitor link group 1, the uplink port GigabitEthernet 1/0/2 is up, and the downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 are up.

Display information about all monitor link groups on Device D.

```
[DeviceD] display monitor-link group all
Monitor link group 1 information:
```

```
  Group status     : UP
  Downlink up-delay: 0(s)
  Last-up-time     : 17:09:33 2019/10/29
  Last-down-time   : -
  Up-port-threshold: 1

  Member                    Role       Status
  ------------------------------------------
  GE1/0/2                   UPLINK     UP
  GE1/0/1                   DOWNLINK   UP
  GE1/0/1                   DOWNLINK   UP
```

The output shows that in monitor link group 1, the uplink port GigabitEthernet 1/0/2 is up, and the downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 are up.

3. Verify the smart link group configuration when GigabitEthernet 1/0/1 on Device A is down:

Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   DOWN    1               17:37:49 2019/10/29
  GE1/0/2                 SECONDARY ACTIVE  4               17:49:06 2019/10/29
```

The output shows that in smart link group 1, the secondary port GigabitEthernet 1/0/2 is active to transmit traffic from VLAN 10.

Display information about the received flush messages on Device C.

```
[DeviceC] display smart-link flush
 Received flush packets                       : 1
 Receiving interface of the last flush packet : GigabitEthernet1/0/2
 Receiving time of the last flush packet      : 17:49:08 2019/10/29
 Device ID of the last flush packet           : 0000-fc00-2500
 Control VLAN of the last flush packet        : 10
```

4. Verify the monitor link group configuration when the uplink port GigabitEthernet 1/0/2 on Device C is down:

Display information about all monitor link groups on Device C.

```
[DeviceC] display monitor-link group all
Monitor link group 1 information:
  Group status     : DOWN
  Downlink up-delay: 0(s)
  Last-up-time     : 17:07:26 2019/10/29
  Last-down-time   : 18:01:05 2019/10/29
  Up-port-threshold: 1

  Member                    Role       Status
```

```
  ----------------------------------------
  GE1/0/2                   UPLINK     DOWN
  GE1/0/1                   DOWNLINK   DOWN (Monitor Link)
  GE1/0/3                   DOWNLINK   DOWN (Monitor Link)
```

The output shows that monitor link group 1 is down, and the downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 in monitor link group 1 are down.

Display information about all monitor link groups on Device D.

```
[DeviceD] display monitor-link group all
Monitor link group 1 information:
  Group status     : UP
  Downlink up-delay: 0(s)
  Last-up-time     : 17:09:33 2019/10/29
  Last-down-time   : -
  Up-port-threshold: 1

  Member                    Role       Status
  ----------------------------------------
  GE1/0/2                   UPLINK     UP
  GE1/0/1                   DOWNLINK   UP
  GE1/0/3                   DOWNLINK   UP
```

The output shows that monitor link group 1 is up, and the downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 in monitor link group 1 are up.

Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 0000-fc00-2500
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   DOWN    2               17:57:49 2019/10/29
  GE1/0/2                 SECONDARY ACTIVE  5               18:01:06 2019/10/29
```

The output shows that GigabitEthernet 1/0/1 on Device A is down. In smart link group 1, the secondary port GigabitEthernet 1/0/2 becomes active to transmit traffic from VLAN 10.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
vlan 1
#
vlan 10
```

```
#
stp region-configuration
 instance 1 vlan 10
active region-configuration
#
smart-link group 1
 preemption mode role
 preemption delay 10
 flush enable control-vlan 10
 protected-vlan reference-instance 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 undo stp enable
 port smart-link group 1 primary
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 undo stp enable
 port smart-link group 1 secondary
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
```

- Device B:

```
#
vlan 1
#
vlan 11
#
stp region-configuration
 instance 1 vlan 11
active region-configuration
#
smart-link group 1
 preemption mode role
 preemption delay 10
 flush enable control-vlan 11
 protected-vlan reference-instance 1
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 undo stp enable
 port smart-link group 1 primary
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 undo stp enable
 port smart-link group 1 secondary
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 11
#
```

- Device C:

```
#
vlan 1
#
vlan 10 to 11
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 undo stp enable
 smart-link flush enable control-vlan 10
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
 port monitor-link group 1 uplink
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 11
 undo stp enable
 smart-link flush enable control-vlan 11
 port monitor-link group 1 downlink
#
```

- Device D:

```
#
vlan 1
#
vlan 10 to 11
#
monitor-link group 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 11
 undo stp enable
 smart-link flush enable control-vlan 11
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
 port monitor-link group 1 uplink
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
 undo stp enable
 smart-link flush enable control-vlan 10
 port monitor-link group 1 downlink
#
```

- Device E:

```
#
vlan 1
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
#
```

Example: Configuring Smart Link in an IRF fabric

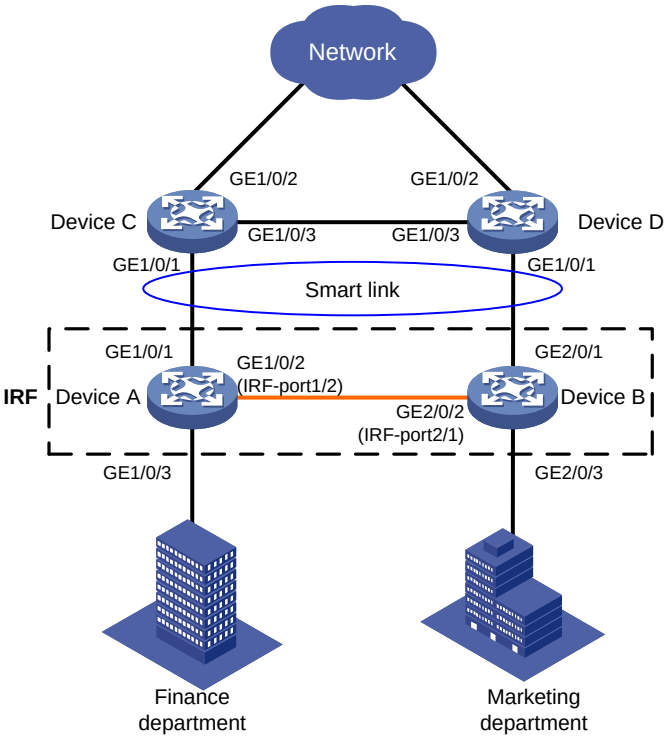
Network configuration

As shown in Figure 3, the Finance department in VLAN 10 and the Marketing department in VLAN 11 are connected to Device A and Device B, respectively. Device A and Device B form an IRF fabric and are connected to Device C and Device D.

Configure Smart Link to meet the following requirements:

- When the uplinks of Device A and Device B are available, traffic is forwarded through the link between Device A and Device C.
- When the link between Device A and Device C fails, the traffic switches to another link.
- When the link recovers, the traffic is switched back to the link.

Figure 3 Network diagram



Device	Interface	VLAN	Device	Interface	Device
Device A	GE1/0/1	10, 11	Device B	GE2/0/1	10, 11
	GE1/0/3	10		GE2/0/3	11
Device C	GE1/0/1	10, 11	Device D	GE1/0/1	10, 11
	GE1/0/2	10, 11		GE1/0/2	10, 11

Analysis

To implement dual uplink redundancy on Device A and Device B, configure a smart link group for the IRF fabric formed by Device A and Device B.

For the traffic to switch back to the recovered link, enable role preemption for the two smart link groups.

For the upstream device to refresh MAC address forwarding entries and ARP/ND entries when link switchover occurs in a smart link group, perform the following tasks:

- Enable flush message sending on Device A and Device B.
- Enable flush message receiving on GigabitEthernet 1/0/1 on Device C and Device D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx

S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure Smart Link in an IRF fabric, follow these restrictions and guidelines:

- Before you configure a port as a smart link group member, shut down the port to prevent loops. You can bring up the port only after completing the smart link group configuration.
- Before you configure a smart link member port or its directly connected port, disable the spann ing tree feature and RRPP on the port.
- Make sure the receive control VLAN configured on the upstream device is the same as the tra nsmit control VLAN configured on the smart link device.

- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.
- For the restrictions and guidelines for configuring IRF, see *HPE xxxx Virtual Technologies Configuration Guide*.

Procedures

Setting up an IRF fabric

Configuring Device A

Bind GigabitEthernet 1/0/2 to IRF port 1/2 and save the configuration.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] shutdown
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface gigabitethernet 1/0/2
[DeviceA-irf-port1/2] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] save
```

Activate the IRF port.

```
[DeviceA] irf-port-configuration active
```

Configuring Device B

Assign IRF member ID 2 to Device B and reboot the device.

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

After you connect the ports as shown in Figure 3, log in to the device again. Bind GigabitEthernet 2/0/2 to IRF port 2/1 and save the configuration.

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] shutdown
[DeviceB-GigabitEthernet2/0/2] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface gigabitethernet 2/0/2
[DeviceB-irf-port2/1] quit
[DeviceB] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] undo shutdown
[DeviceB-GigabitEthernet2/0/2] quit
[DeviceB] save
```

Activate the IRF port.

```
[DeviceB] irf-port-configuration active
```

Device A and Device B start a master election. When the master (Device A in this example) is elected, the other device reboots. An IRF fabric is formed after the reboot.

Configuring Smart Link

Configuring Device A

1. Create VLAN 10 and VLAN 11.

```
<DeviceA> system-view
[DeviceA] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Shut down GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] shutdown
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 2/0/1 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] shutdown
[DeviceA-GigabitEthernet2/0/1] port link-type trunk
[DeviceA-GigabitEthernet2/0/1] port trunk permit vlan 10 11
[DeviceA-GigabitEthernet2/0/1] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet2/0/1] undo stp enable
[DeviceA-GigabitEthernet2/0/1] quit
```

4. Configure GigabitEthernet 1/0/3:

Configure GigabitEthernet 1/0/3 as an access port and assign the port to VLAN 10.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port access vlan 10
```

Bring up the port.

```
[DeviceA-GigabitEthernet1/0/3] undo shutdown
[DeviceA-GigabitEthernet1/0/3] quit
```

5. Configure GigabitEthernet 2/0/3:

Configure GigabitEthernet 2/0/3 as an access port and assign the port to VLAN 11.

```
[DeviceA] interface gigabitethernet 2/0/3
[DeviceA-GigabitEthernet2/0/3] port access vlan 11
```

Bring up the port.

```
[DeviceA-GigabitEthernet2/0/3] undo shutdown
[DeviceA-GigabitEthernet2/0/3] quit
```

6. Configure VLAN-to-MSTI mappings and activate the MST region configuration::

Enter MST region view.

```
[DeviceA] stp region-configuration
```

Map VLAN 10 and VLAN 11 to MSTI 1.

```
[DeviceA-mst-region] instance 1 vlan 10 11
```

Activate the MST region configuration

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

7. Configure smart link group 1:

Create smart link group 1 and configure the VLANs mapped to MSTI 1, VLAN 10 and VLAN 11, as the protected VLANs.

```
[DeviceA] smart-link group 1
[DeviceA-smlk-group1] protected-vlan reference-instance 1
```

Configure GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 2/0/1 as the secondary port.

```
[DeviceA-smlk-group1] port gigabitethernet 1/0/1 primary
[DeviceA-smlk-group1] port gigabitethernet 2/0/1 secondary
```

Enable flush message sending, and configure VLAN 10 as the transmit control VLAN.

```
[DeviceA-smlk-group1] flush enable control-vlan 10
```

Enable role preemption and set the preemption delay to 10 seconds.

```
[DeviceA-smlk-group1] preemption mode role
[DeviceA-smlk-group1] preemption delay 10
[DeviceA-smlk-group1] quit
```

8. Bring up GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1:

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] undo shutdown
[DeviceA-GigabitEthernet2/0/1] quit
```

Configuring Device C

1. Create VLAN 10 and VLAN 11.

```
<DeviceC> system-view
[DeviceC] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLAN 10 and VLAN 11.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
```

Enable flush message receiving, and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceC-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
```

Bring up the port.

```
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

   # Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
```

   # Assign the port to VLAN 10 and VLAN 11.

```
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

   # Remove the port from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

   # Enable flush message receiving, and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceC-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

   # Bring up the port.

```
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring Device D

1. Create VLAN 10 and VLAN 11.

```
<DeviceD> system-view
[DeviceD] vlan 10 to 11
```

2. Configure GigabitEthernet 1/0/1:

   # Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

   # Assign the port to VLAN 10 and VLAN 11.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 10 11
```

   # Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

   # Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
```

   # Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/1] smart-link flush enable control-vlan 10 11
```

   # Bring up the port.

```
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] quit
```

3. Configure GigabitEthernet 1/0/2:

   # Configure GigabitEthernet 1/0/2 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
```

   # Assign the port to VLAN 10 and VLAN 11.

```
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 10 11
```

   # Remove the port from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

   # Enable flush message receiving and configure VLAN 10 and VLAN 11 as the receive control VLANs on the port.

```
[DeviceD-GigabitEthernet1/0/2] smart-link flush enable control-vlan 10 11
```

   # Bring up the port.

```
[DeviceD-GigabitEthernet1/0/2] undo shutdown
```

```
[DeviceD-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify the IRF fabric configuration after you complete the configuration:

   # Display IRF fabric information on Device A.

```
<Sysname> display irf
MemberID  Role     Priority    CPU-Mac           Description
 *+1      Master   1           0210-fc01-0001    -----
   2      Standby  1           0210-fc02-0002    -----
-------------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 00e0-fc00-1000
 Auto upgrade                  : yes
 Mac persistent                : 6 min
 Domain ID                     : 0
```

   The output shows that an IRF fabric has been established successfully.

2. Verify the smart link group configuration when Device A is operating correctly:

   # Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 00e0-fc00-c518
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1
  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   ACTIVE  3               18:16:44 2019/10/29
  GE2/0/1                 SECONDARY STANDBY 0               NA
```

   The output shows that in smart link group 1, the primary port GigabitEthernet 1/0/1 is active to transmit traffic from VLAN 10 and VLAN 11.

3. Verify the smart link group configuration when GigabitEthernet 1/0/1 on Device A is down.

   # Display information about all smart link groups on Device A.

```
[DeviceA] display smart-link group all
Smart link group 1 information:
  Device ID       : 00e0-fc00-c518
  Preemption mode : Role
  Preemption delay: 10(s)
  Control VLAN    : 10
  Protected VLAN  : Reference Instance 1

  Member                  Role      State   Flush-count     Last-flush-time
  ------------------------------------------------------------------------------
  GE1/0/1                 PRIMARY   DOWN    3               18:16:44 2019/10/29
```

```
  GE2/0/1                 SECONDARY ACTIVE  1              18:22:37 2019/10/29
```

The output shows that in smart link group 1, the secondary port GigabitEthernet 2/0/1 is active to transmit traffic for VLAN 10 and VLAN 11.

Display information about the received flush messages on Device C.

```
[DeviceC] display smart-link flush
 Received flush packets                       : 1
 Receiving interface of the last flush packet : GigabitEthernet1/0/3
 Receiving time of the last flush packet      : 18:22:39 2019/10/29
 Device ID of the last flush packet           : 00e0-fc00-c518
 Control VLAN of the last flush packet        : 10
```

Display information about the received flush messages on Device D.

```
[DeviceD] display smart-link flush
 Received flush packets                       : 1
 Receiving interface of the last flush packet : GigabitEthernet1/0/1
 Receiving time of the last flush packet      : 18:22:38 2019/10/29
 Device ID of the last flush packet           : 00e0-fc00-c518
 Control VLAN of the last flush packet        : 10
```

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
vlan 10 to 11
#
 irf mac-address persistent always
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
 irf member 2 priority 1
#
irf-port 1/2
 port group interface GigabitEthernet1/0/2
#
irf-port 2/1
 port group 1 interface GigabitEthernet2/0/2
#
stp region-configuration
 instance 1 vlan 10 to 11
 active region-configuration
#
smart-link group 1
 preemption mode role
 preemption delay 10
```

```
 flush enable control-vlan 10
 protected-vlan reference-instance 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 port smart-link group 1 primary
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
port smart-link group 1 secondary
#
interface GigabitEthernet2/0/3
 port link-mode bridge
 port access vlan 11
#
```

- Device C:

```
#
 sysname DeviceC
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
```

```
#
```

- Device D:

```
#
 sysname DeviceD
#
vlan 10 to 11
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 undo stp enable
 smart-link flush enable control-vlan 10 to 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 to 11
 smart-link flush enable control-vlan 10 to 11
#
```

Contents

Introduction

This document provides RRPP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of RRPP.

General restrictions and guidelines

When you configure RRPP, follow these restrictions and guidelines:

- Do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN.
- On swiches that support QinQ and VLAN mapping, do not enable QinQ or VLAN mapping on control VLANs. If you do, RRPPDUs cannot be correctly forwarded.
- On swiches that support Layer 3 Ethernet interfaces, the primary and secondary control VLAN IDs must be different from the Layer 3 Ethernet subinterface IDs of the master ring and subrings.
- To prevent temporary broadcast storms, do not enable the OAM remote loopback feature on an RRPP port.

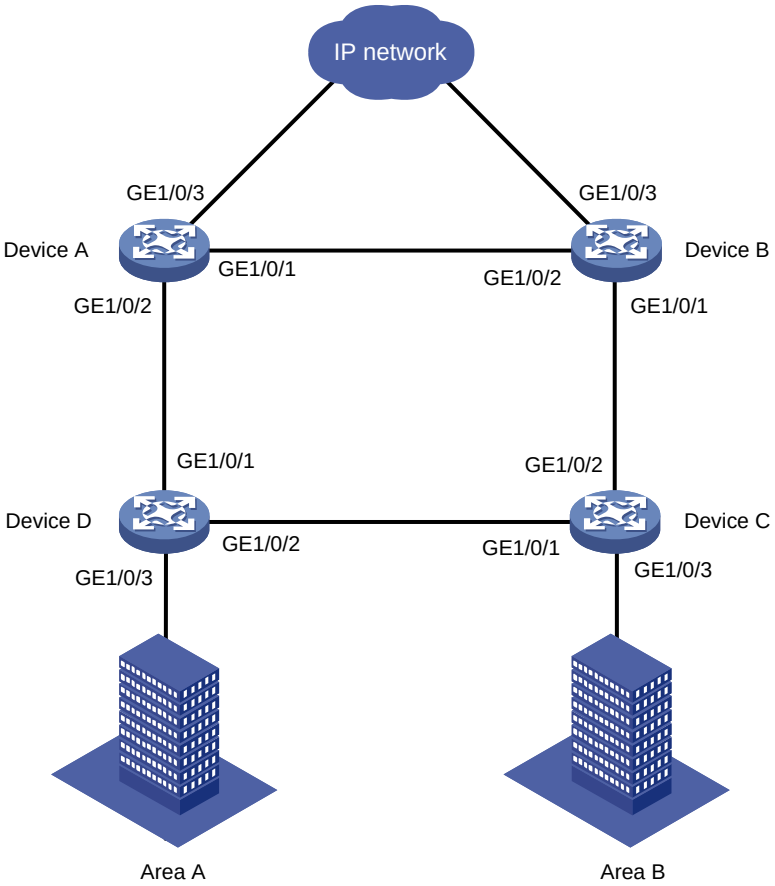
Example: Configuring a single ring

Network configuration

As shown in Figure 1, area A and area B are connected to a ring-shaped distribution layer network. Configure RRPP to implement the following requirements in the network:

- Eliminate loops and implement link recovery in the Layer 2 network.
- Implement link load balancing by forwarding voice traffic in VLAN 100 through VLAN 150 and video traffic in VLAN 151 through VLAN 200.
- Improve RRPP topology convergence speed by setting the physical state change suppression interval to 0 seconds for all Ethernet interfaces on the RRPP ring.

Figure 1 Network diagram



Analysis

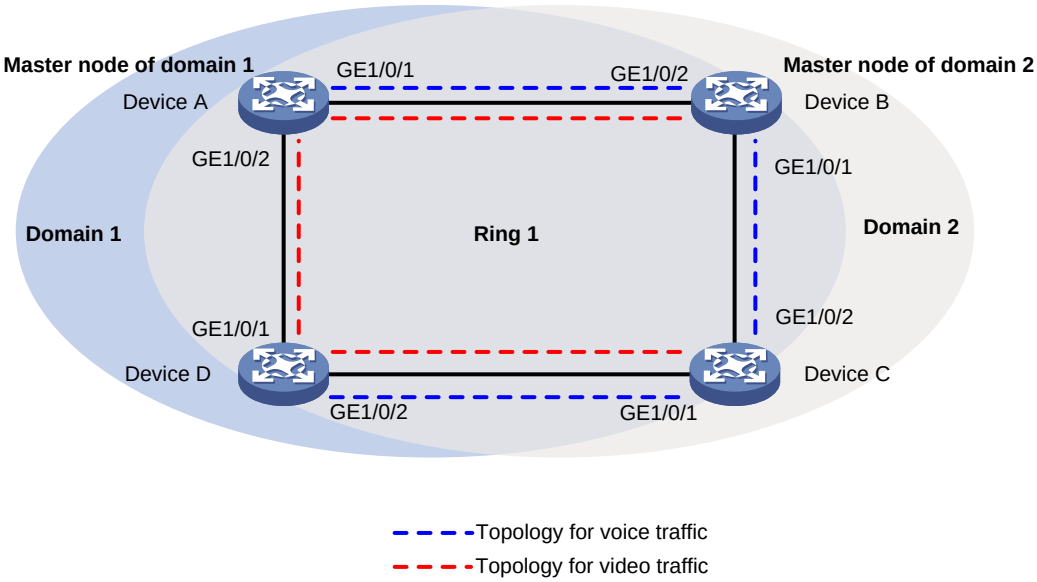
For voice and video traffic to be forwarded in different topologies, create two RRPP domains.

- In RRPP domain 1, specify VLAN 100 through VLAN 150 as protected VLANs, and specify Device A as the master node.
- In RRPP domain 2, specify VLAN 151 through VLAN 200 as protected VLANs, and specify Device B as the master node.

To implement load balancing for voice and video traffic, perform the following tasks:

- On Device A, specify GigabitEthernet 1/0/1 as the primary port, and GigabitEthernet 1/0/2 as the secondary port.
- On Device B, specify GigabitEthernet 1/0/2 as the primary port, and GigabitEthernet 1/0/1 as the secondary port.

Figure 2 Topologies for voice and video traffic



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx,

S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series	Release 63xx

MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure a single RRPP ring, follow these restrictions and guidelines:

- After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. You can only use the **undo control-vlan** command to delete a primary control VLAN.
- When you configure load balancing, you must configure different protected VLANs for different RRPP domains.
- When you configure RRPP port roles, disable the spanning tree feature on the ports, and make sure the ports are not member ports of any smart link groups.

Procedures

Configuring Device A

Create VLANs 100 through 200.

```
<DeviceA> system-view
[DeviceA] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 100 to 150
[DeviceA-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceA-GigabitEthernet1/0/1] link-delay up 0
[DeviceA-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] link-delay up 0
[DeviceA-GigabitEthernet1/0/2] link-delay down 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceA] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceA-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device A as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

Create VLANs 100 through 200.

```
<DeviceB> system-view
[DeviceB] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 100 to 150
[DeviceB-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceB-GigabitEthernet1/0/1] link-delay up 0
[DeviceB-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] link-delay up 0
[DeviceB-GigabitEthernet1/0/2] link-delay down 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain1] ring 1 enable
```

```
[DeviceB-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device B as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain2] ring 1 enable
[DeviceB-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

Create VLANs 100 through 200.

```
<DeviceC> system-view
[DeviceC] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 100 to 150
[DeviceC-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceC-GigabitEthernet1/0/1] link-delay up 0
[DeviceC-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
```

```
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] link-delay up 0
[DeviceC-GigabitEthernet1/0/2] link-delay down 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
[DeviceC-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceC] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceC-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
[DeviceC-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

Create VLANs 100 through 200.

```
<DeviceD> system-view
[DeviceD] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 100 to 150
[DeviceD-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
```

```
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceD-GigabitEthernet1/0/1] link-delay up 0
[DeviceD-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] link-delay up 0
[DeviceD-GigabitEthernet1/0/2] link-delay down 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceD] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceD-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Verifying the configuration

View detailed information about RRPP domain 1 on Device A.

```
[DeviceA] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: BLOCKED
```

The output shows the following information:

- Device A is the master node in RRPP domain 1.
- The primary ring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device A.

```
[DeviceA] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP
```

The output shows the following information:

- Device A is the transit node in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device B.

```
[DeviceB] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: UP
```

The output shows the following information:

- Device B is the transit node in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device B.

```
[DeviceB] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: BLOCKED
```

The output shows the following information:

- Device B is the master node in RRPP domain 2.
- The primary ring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 1 on Device C.

```
[DeviceC] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
```

```
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP
```

The output shows the following information:

- Device C is the transit node in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device C.

```
[DeviceC] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP
```

The output shows the following information:

- Device C is the transit node in RRPP domain 2.
- The primary and secondary ports are up.

View detailed RRPP domain information on Device D. (Details not shown.)

Configuration files

NOTE:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
vlan 1
#
```

```
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
 sysname DeviceB
#
vlan 1
#
vlan 100 to 200
#
```

```
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device C:

```
#
 sysname DeviceC
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
```

```
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device D:

```
#
 sysname DeviceD
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

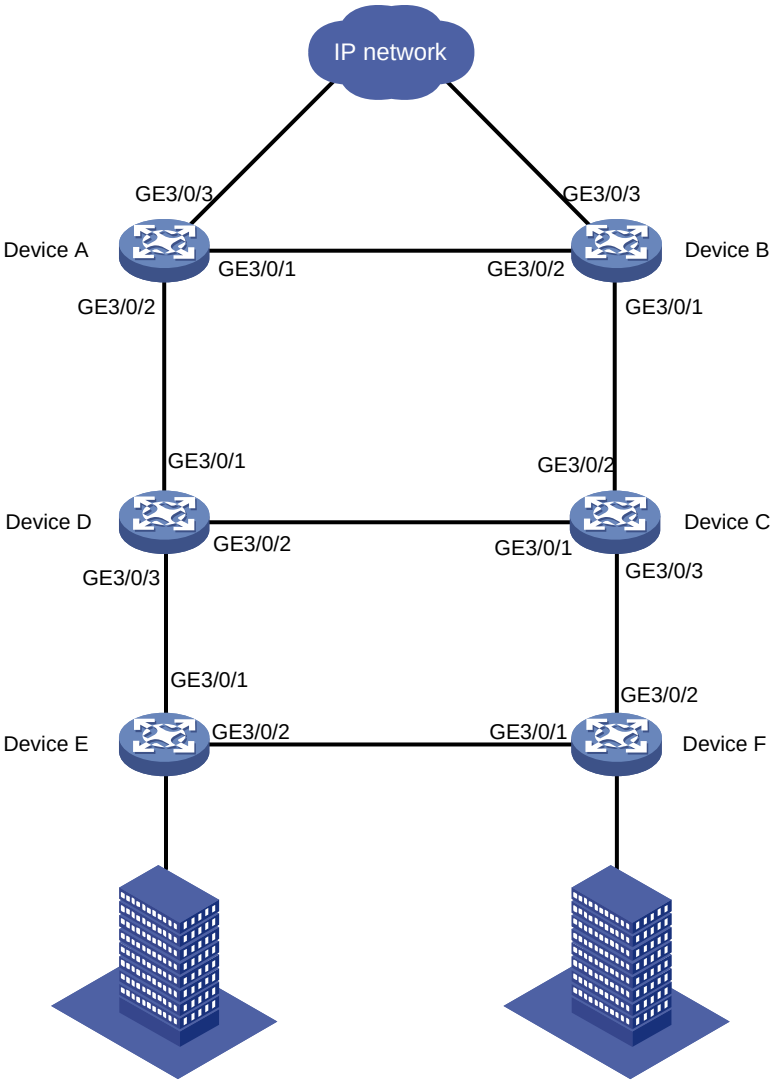
Example: Configuring intersecting rings

Network configuration

As shown in Figure 3, a ring-shaped access layer network is connected to a ring-shaped distribution layer network. Configure RRPP to implement the following requirements in the network:

- Eliminate loops and implement link recovery in the Layer 2 network.
- Implement link load balancing by forwarding voice traffic in VLAN 100 through VLAN 150 and video traffic in VLAN 151 through VLAN 200.
- Improve RRPP topology convergence speed by setting the physical state change suppression interval to 0 seconds for all Ethernet interfaces on the RRPP ring.

Figure 3 Network diagram



Analysis

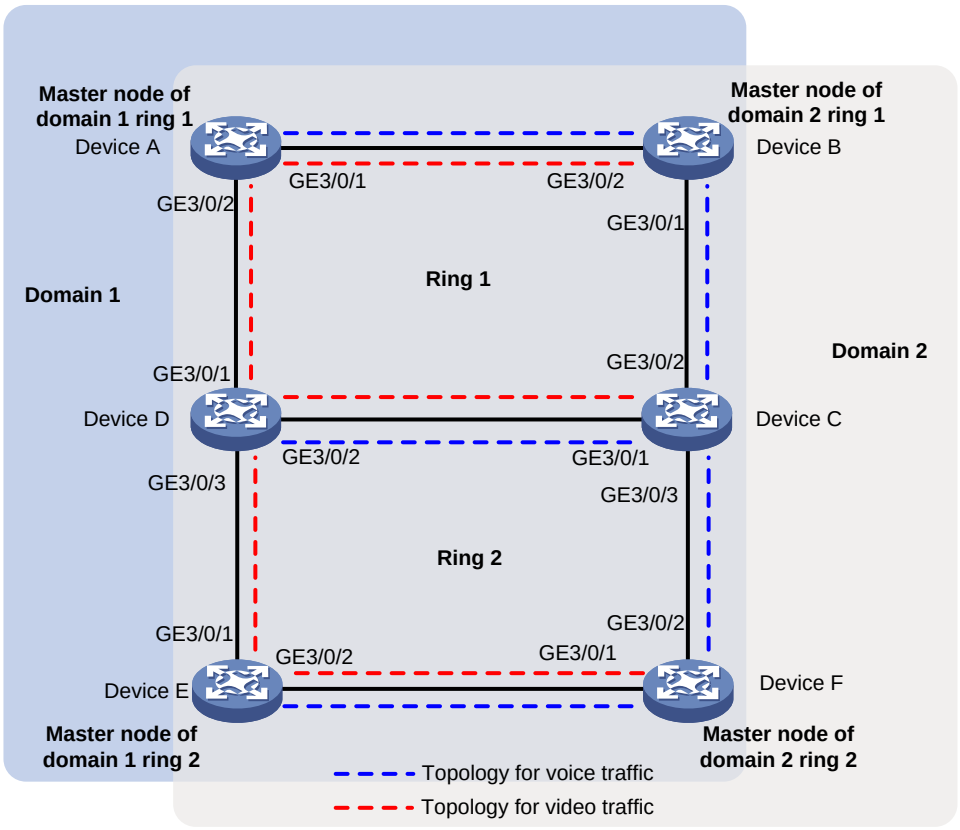
For voice and video traffic to be forwarded in different topologies, create two RRPP domains.

- In RRPP domain 1, specify VLAN 100 through VLAN 150 as protected VLANs. Specify Device A as the master node of primary ring 1, and Device E as the master node of subring 2.
- In RRPP domain 2, specify VLAN 151 through VLAN 200 as protected VLANs. Specify Device B as the master node of primary ring 1, and Device F as the master node of subring 2.

To implement load balancing for voice and video traffic, perform the following tasks:

- On Device A, specify GigabitEthernet 1/0/1 as the primary port, and GigabitEthernet 1/0/2 as the secondary port.
- On Device B, specify GigabitEthernet 1/0/2 as the primary port, and GigabitEthernet 1/0/1 as the secondary port.
- On Device E, specify GigabitEthernet 1/0/2 as the primary port, and GigabitEthernet 1/0/1 as the secondary port.
- On Device F, specify GigabitEthernet 1/0/1 as the primary port, and GigabitEthernet 1/0/2 as the secondary port.

Figure 4 Topologies for voice and video traffic



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

MS4520V2-54C switch	
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series	Not supported

S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure intersecting rings, follow these restrictions and guidelines:

- When you configure an edge node or assistant edge node, you must configure the primary ring before configuring the subrings.
- After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. You can only use the **undo control-vlan** command to delete a primary control VLAN.
- When you configure load balancing, you must configure different protected VLANs for different RRPP domains.
- Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings.
- If a device carries multiple RRPP rings in an RRPP domain, it can only be an edge node or an assistant edge node on a subring.
- To prevent Hello packets of subrings from being looped on the primary ring, first enable the primary ring on its master node. Then enable the subrings on their respective master nodes.

Procedures

Configuring Device A

Create VLANs 100 through 200.

```
<DeviceA> system-view
```

```
[DeviceA] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 100 to 150
[DeviceA-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceA-GigabitEthernet1/0/1] link-delay up 0
[DeviceA-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] link-delay up 0
[DeviceA-GigabitEthernet1/0/2] link-delay down 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceA] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceA-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device A as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

Create VLANs 100 through 200.

```
<DeviceB> system-view
[DeviceB] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 100 to 150
[DeviceB-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceB-GigabitEthernet1/0/1] link-delay up 0
[DeviceB-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] link-delay up 0
[DeviceB-GigabitEthernet1/0/2] link-delay down 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device B as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain2] ring 1 enable
[DeviceB-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

Create VLANs 100 through 200.

```
<DeviceC> system-view
[DeviceC] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 100 to 150
[DeviceC-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] undo shutdown
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
```

```
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceC-GigabitEthernet1/0/1] link-delay up 0
[DeviceC-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceC-GigabitEthernet1/0/1] undo stp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] undo shutdown
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] link-delay up 0
[DeviceC-GigabitEthernet1/0/2] link-delay down 0
[DeviceC-GigabitEthernet1/0/2] undo stp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] undo shutdown
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 100 to 200
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] link-delay up 0
[DeviceC-GigabitEthernet1/0/3] link-delay down 0
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] quit
```

Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

Configure Device C as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceC-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceC] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceC-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

Configure Device C as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable
[DeviceC-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

Create VLANs 100 through 200.

```
<DeviceD> system-view
[DeviceD] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 100 to 150
[DeviceD-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] undo shutdown
[DeviceD-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceD-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceD-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceD-GigabitEthernet1/0/1] link-delay up 0
[DeviceD-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceD-GigabitEthernet1/0/1] undo stp enable
[DeviceD-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/2
[DeviceD-GigabitEthernet1/0/2] undo shutdown
[DeviceD-GigabitEthernet1/0/2] port link-type trunk
[DeviceD-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
```

```
[DeviceD-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/2] link-delay up 0
[DeviceD-GigabitEthernet1/0/2] link-delay down 0
[DeviceD-GigabitEthernet1/0/2] undo stp enable
[DeviceD-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] undo shutdown
[DeviceD-GigabitEthernet1/0/3] port link-type trunk
[DeviceD-GigabitEthernet1/0/3] port trunk permit vlan 100 to 200
[DeviceD-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceD-GigabitEthernet1/0/3] link-delay up 0
[DeviceD-GigabitEthernet1/0/3] link-delay down 0
[DeviceD-GigabitEthernet1/0/3] undo stp enable
[DeviceD-GigabitEthernet1/0/3] quit
```

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

Configure Device D as the assistant edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceD-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 2 enable
[DeviceD-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceD] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceD-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
```

Configure Device D as the assistant edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceD-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain2] ring 2 enable
[DeviceD-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Configuring Device E

Create VLANs 100 through 200.

```
<DeviceE> system-view
[DeviceE] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 100 to 150
[DeviceE-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceE-GigabitEthernet1/0/1] link-delay up 0
[DeviceE-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] link-delay up 0
[DeviceE-GigabitEthernet1/0/2] link-delay down 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceE] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceE-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceE] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceE-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device E as the transit node of subring 2, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 2.

```
[DeviceE-rrpp-domain2] ring 2 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceE] rrpp enable
```

Configuring Device F

Create VLANs 100 through 200.

```
<DeviceF> system-view
[DeviceF] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 100 to 150
[DeviceF-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo shutdown
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceF-GigabitEthernet1/0/1] link-delay up 0
[DeviceF-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
```

```
[DeviceF-GigabitEthernet1/0/2] undo shutdown
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] link-delay up 0
[DeviceF-GigabitEthernet1/0/2] link-delay down 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceF] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceF-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device F as the transit node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.

```
[DeviceF-rrpp-domain1] ring 2 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain1] ring 2 enable
[DeviceF-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceF] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceF-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceF-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device F as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.

```
[DeviceF-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain2] ring 2 enable
[DeviceF-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceF] rrpp enable
```

Verifying the configuration

View detailed information about RRPP domain 1 on Device A.

```
[DeviceA] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
```

```
 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: BLOCKED
```

The output shows the following information:

- Device A is the master node of primary ring 1 in RRPP domain 1.
- The primary ring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device A.

```
[DeviceA] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP
```

The output shows the following information:

- Device A is the transit node of primary ring 1 in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device B.

```
[DeviceB] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
```

```
 Secondary port: GE1/0/1                    Port status: UP
```

The output shows the following information:

- Device B is the transit node of primary ring 1 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device B.

```
[DeviceB] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                    Port status: UP
 Secondary port: GE1/0/1                    Port status: BLOCKED
```

The output shows the following information:

- Device B is the master node of primary ring 1 in RRPP domain 2.
- The primary ring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 1 on Device C.

```
[DeviceC] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                    Port status: UP
 Secondary port: GE1/0/2                    Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Edge
 Ring State    : -
```

```
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP
```

The output shows the following information:

- Device C is the transit node of primary ring 1 and edge node of subring 2 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device C.

```
[DeviceC] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

Ring ID       : 1
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Enable Status : Yes    Active Status: Yes
Primary port  : GE1/0/1                   Port status: UP
Secondary port: GE1/0/2                   Port status: UP

Ring ID       : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : -
Enable Status : Yes    Active Status: Yes
Common port   : GE1/0/1                   Port status: UP
                GE1/0/2                   Port status: UP
Edge port     : GE1/0/3                   Port status: UP
```

The output shows the following information:

- Device C is the transit node of primary ring 1 and edge node of subring 2 in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device D.

```
[DeviceD] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
```

```
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 1 and assistant edge node of subring 2 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device D.

```
[DeviceD] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 1 and assistant edge node of subring 2 in RRPP domain 2.

- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device E.

```
[DeviceE] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: BLOCKED
```

The output shows the following information:

- Device E is the master node of subring 2 in RRPP domain 1.
- The subring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device E.

```
[DeviceE] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: UP
```

The output shows the following information:

- Device E is the transit node of subring 2 in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device F.

```
[DeviceF] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
```

```
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP
```

The output shows the following information:

- Device F is the transit node of subring 2 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device F.

```
[DeviceF] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: BLOCKED
```

The output shows the following information:

- Device F is the master node of subring 2 in RRPP domain 2.
- The subring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

Configuration files

NOTE:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
```

```
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
 sysname DeviceB
#
vlan 1
```

```
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device C:

```
#
 sysname DeviceC
#
vlan 1
#
vlan 100 to 200
```

```
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
```

```
 ring 2 enable
#
rrpp enable
#
```

- Device D:

```
#
 sysname DeviceD
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
```

```
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
#
rrpp enable
#
```

- Device E:

```
#
 sysname DeviceE
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
```

```
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
 ring 2 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 2 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
 ring 2 enable
#
rrpp enable
#
```

- Device F:

```
#
 sysname DeviceF
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
```

```
 ring 2 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp enable
#
```

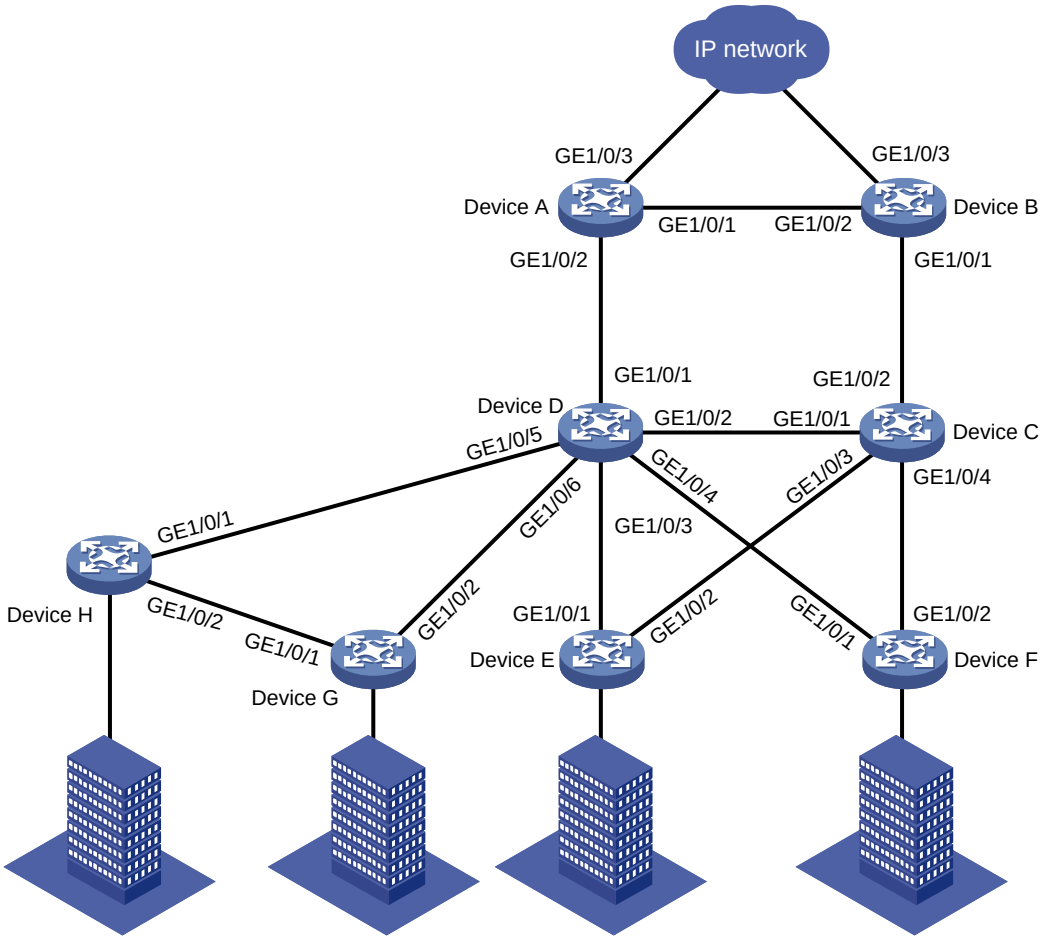
Example: Configuring dual-homed intersecting rings

Network configuration

As shown in Figure 5, a ring-shaped campus network is connected to a ring-shaped distribution layer network through an access layer device. Configure RRPP to implement the following requirements in the network:

- Eliminate loops and implement link recovery in the Layer 2 network.
- Implement link load balancing by forwarding voice traffic in VLAN 100 through VLAN 150 and video traffic in VLAN 151 through VLAN 200.
- Improve RRPP topology convergence speed by setting the physical state change suppression interval to 0 seconds for all Ethernet interfaces on the RRPP ring.
- Reduce the number of Edge-Hello packets.

Figure 5 Network diagram



Analysis

For voice and video traffic to be forwarded in different topologies, create four RRPP domains.

- In RRPP domain 1 and domain 4, specify VLAN 100 through VLAN 150 as protected VLANs, and configure the node roles as follows:
  - Specify Device A as the master node of primary ring 1.
  - Specify Device E as the master node of subring 2.
  - Specify Device F as the master node of subring 3.
  - Specify Device H as the master node of subring 4.
- In RRPP domain 2 and domain 3, specify VLAN 151 through VLAN 200 as protected VLANs, and configure the node roles as follows:
  - Specify Device B as the master node of primary ring 1.
  - Specify Device E as the master node of subring 2.
  - Specify Device F as the master node of subring 3.
  - Specify Device H as the master node of subring 4.

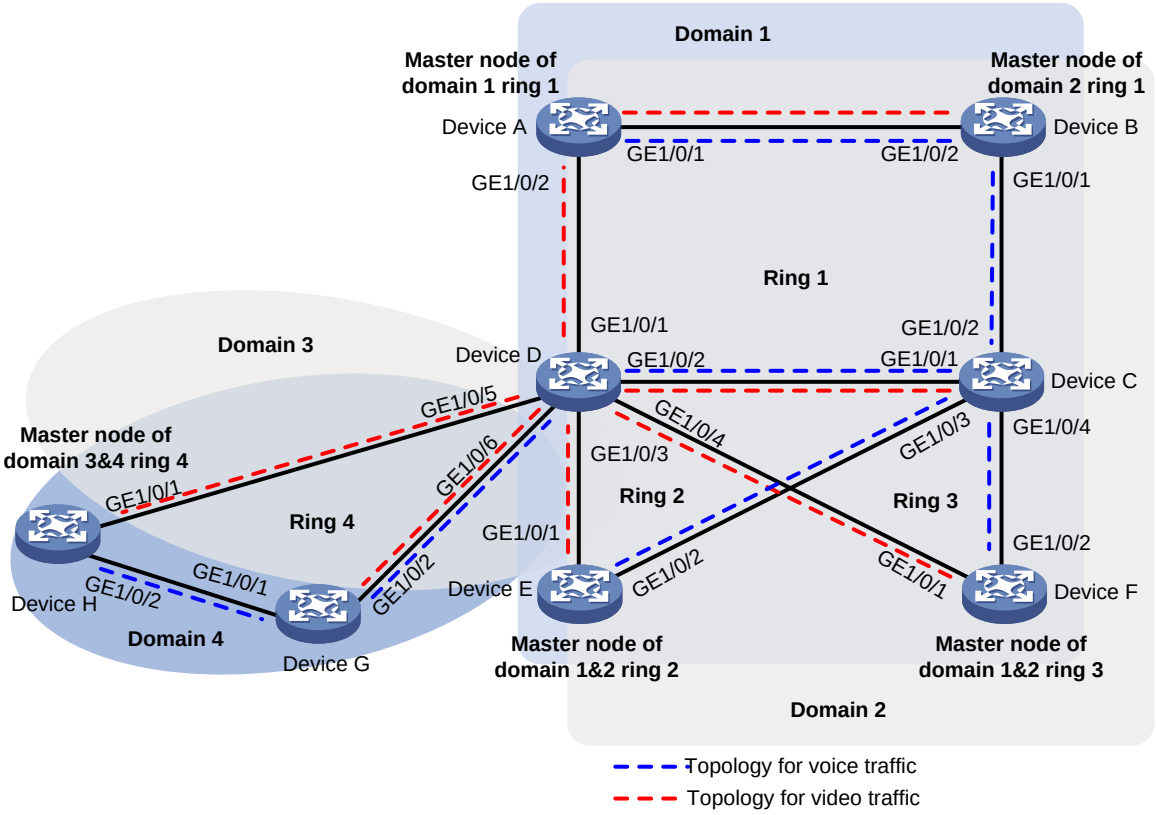
To implement load balancing for voice and video traffic, perform the following tasks:

- On Device A, specify GigabitEthernet 1/0/1 as the primary port, and GigabitEthernet 1/0/2 as the secondary port.

- On Device B, specify GigabitEthernet 1/0/2 as the primary port, and GigabitEthernet 1/0/1 as the secondary port.
- On Device E, specify GigabitEthernet 1/0/1 as the secondary port in RRPP domain 1 and primary port in RRPP domain 2. Specify GigabitEthernet 1/0/2 as the primary port in RRPP domain 1 and secondary port in RRPP domain 2.
- On Device F, specify GigabitEthernet 1/0/1 as the secondary port in RRPP domain 1 and primary port in RRPP domain 2. Specify GigabitEthernet 1/0/2 as the primary port in RRPP domain 1 and secondary port in RRPP domain 2.
- On Device H, specify GigabitEthernet 1/0/1 as the primary port in RRPP domain 3 and secondary port in RRPP domain 4. Specify GigabitEthernet 1/0/2 as the secondary port in RRPP domain 3 and primary port in RRPP domain 4.

To reduce the number of Edge-Hello packets, add ring 2 and ring 3 in RRPP domain 1 and 2 to a ring group.

Figure 6 Topologies for voice and video traffic



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx

S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure dual-homed intersecting rings, follow these restrictions and guidelines:

- To avoid temporary loops when the primary ring fails, make sure the difference between the Fail timer values on the master node of the subring and primary ring is greater than twice the Hello timer value on the master node of the subring.
- When you configure an edge node or assistant edge node, you must configure the primary ring before configuring the subrings.
- After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. You can only use the **undo control-vlan** command to delete a primary control VLAN.

- When you configure load balancing, you must configure different protected VLANs for different RRPP domains.
- Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings.
- If a device carries multiple RRPP rings in an RRPP domain, it can only be an edge node or an assistant edge node on a subring.
- To prevent Hello packets of subrings from being looped on the primary ring, first enable the primary ring on its master node. Then enable the subrings on their respective master nodes.
- Make sure all subrings in an RRPP ring group have the same SRPTs. You can assign a subring to only one RRPP ring group. For the RRPP ring group to operate correctly, the RRPP ring groups configured on the edge node and the assistant edge node must contain the same subrings.
- Make sure the RRPP ring groups on the edge node and the assistant edge node have the same configurations and activation status.

Procedures

Configuring Device A

Create VLANs 100 through 200.

```
<DeviceA> system-view
[DeviceA] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 100 to 150
[DeviceA-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] undo shutdown
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceA-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceA-GigabitEthernet1/0/1] link-delay up 0
[DeviceA-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceA-GigabitEthernet1/0/1] undo stp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] undo shutdown
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
```

```
[DeviceA-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/2] link-delay up 0
[DeviceA-GigabitEthernet1/0/2] link-delay down 0
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceA] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceA-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device A as the master node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceA] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceA-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device A as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceA-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceA] rrpp enable
```

Configuring Device B

Create VLANs 100 through 200.

```
<DeviceB> system-view
[DeviceB] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 100 to 150
[DeviceB-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] undo shutdown
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceB-GigabitEthernet1/0/1] link-delay up 0
[DeviceB-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceB-GigabitEthernet1/0/1] undo stp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] undo shutdown
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceB-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/2] link-delay up 0
[DeviceB-GigabitEthernet1/0/2] link-delay down 0
[DeviceB-GigabitEthernet1/0/2] undo stp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceB] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceB-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device B as the transit node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceB] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceB-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device B as the master node of primary ring 1, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 1.

```
[DeviceB-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceB-rrpp-domain2] ring 1 enable
[DeviceB-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceB] rrpp enable
```

Configuring Device C

Create VLANs 100 through 200.

```
<DeviceC> system-view
[DeviceC] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 1 vlan 100 to 150
[DeviceC-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 as trunk ports.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceC-if-range] undo shutdown
[DeviceC-if-range] port link-type trunk
```

Assign the ports to VLANs 100 through 200, and remove them from VLAN 1.

```
[DeviceC-if-range] port trunk permit vlan 100 to 200
[DeviceC-if-range] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the ports.

```
[DeviceC-if-range] link-delay up 0
[DeviceC-if-range] link-delay down 0
```

Disable the spanning tree feature on the ports.

```
[DeviceC-if-range] undo stp enable
[DeviceC-if-range] quit
```

Create RRPP domain 1.

```
[DeviceC] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceC-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain1] ring 1 enable
```

Configure Device C as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceC-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain1] ring 2 enable
```

Configure Device C as the edge node of subring 3, with GigabitEthernet 1/0/4 as the edge port. Enable ring 3.

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain1] ring 3 enable
```

```
[DeviceC-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceC] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceC-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device C as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceC-rrpp-domain2] ring 1 enable
```

Configure Device C as the edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
[DeviceC-rrpp-domain2] ring 2 enable
```

Configure Device C as the edge node of subring 3, with GigabitEthernet 1/0/4 as the edge port. Enable ring 3.

```
[DeviceC-rrpp-domain2] ring 3 node-mode edge edge-port gigabitethernet 1/0/4
[DeviceC-rrpp-domain2] ring 3 enable
[DeviceC-rrpp-domain2] quit
```

Create RRPP ring group 1, and add subrings 2 and 3 in RRPP domains 1 and 2 to the RRPP ring group.

```
[DeviceC] rrpp ring-group 1
[DeviceC-ring-group1] domain 1 ring 2 3
[DeviceC-ring-group1] domain 2 ring 2 3
[DeviceC-ring-group1] quit
```

Enable RRPP.

```
[DeviceC] rrpp enable
```

Configuring Device D

Create VLANs 100 through 200.

```
<DeviceD> system-view
[DeviceD] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] instance 1 vlan 100 to 150
[DeviceD-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

Configure GigabitEthernet 1/0/1 through GigabitEthernet 1/0/6 as trunk ports.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[DeviceD-if-range] undo shutdown
[DeviceD-if-range] port link-type trunk
```

Assign the ports to VLANs 100 through 200, and remove them from VLAN 1.

```
[DeviceD-if-range] port trunk permit vlan 100 to 200
[DeviceD-if-range] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the ports.

```
[DeviceD-if-range] link-delay up 0
[DeviceD-if-range] link-delay down 0
```

Disable the spanning tree feature on the ports.

```
[DeviceD-if-range] undo stp enable
[DeviceD-if-range] quit
```

Create RRPP domain 1.

```
[DeviceD] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceD-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
```

Configure Device D as the assistant edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceD-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain1] ring 2 enable
```

Configure Device D as the assistant edge node of subring 3, with GigabitEthernet 1/0/4 as the edge port. Enable ring 3.

```
[DeviceD-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain1] ring 3 enable
[DeviceD-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceD] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceD-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device D as the transit node of primary ring 1, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 1.

```
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
```

Configure Device D as the assistant edge node of subring 2, with GigabitEthernet 1/0/3 as the edge port. Enable ring 2.

```
[DeviceD-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
[DeviceD-rrpp-domain2] ring 2 enable
```

Configure Device D as the assistant edge node of subring 3, with GigabitEthernet 1/0/4 as the edge port. Enable ring 3.

```
[DeviceD-rrpp-domain2] ring 3 node-mode assistant-edge edge-port gigabitethernet 1/0/4
[DeviceD-rrpp-domain2] ring 3 enable
[DeviceD-rrpp-domain2] quit
```

Create RRPP domain 3.

```
[DeviceD] rrpp domain 3
```

Configure VLAN 3000 as the primary control VLAN of RRPP domain 3.

```
[DeviceD-rrpp-domain3] control-vlan 3000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 3.

```
[DeviceD-rrpp-domain3] protected-vlan reference-instance 1
```

Configure Device D as the transit node of primary ring 4, with GigabitEthernet 1/0/5 as the primary port and GigabitEthernet 1/0/6 as the secondary port. Enable ring 4.

```
[DeviceD-rrpp-domain3] ring 4 node-mode transit primary-port gigabitethernet 1/0/5
secondary-port gigabitethernet 1/0/6 level 0
[DeviceD-rrpp-domain3] ring 4 enable
[DeviceD-rrpp-domain3] quit
```

Create RRPP domain 4.

```
[DeviceD] rrpp domain 4
```

Configure VLAN 4000 as the primary control VLAN of RRPP domain 4.

```
[DeviceD-rrpp-domain4] control-vlan 4000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 4.

```
[DeviceD-rrpp-domain4] protected-vlan reference-instance 2
```

Configure Device D as the transit node of primary ring 4, with GigabitEthernet 1/0/5 as the primary port and GigabitEthernet 1/0/6 as the secondary port. Enable ring 4.

```
[DeviceD-rrpp-domain4] ring 4 node-mode transit primary-port gigabitethernet 1/0/5
secondary-port gigabitethernet 1/0/6 level 0
[DeviceD-rrpp-domain4] ring 4 enable
[DeviceD-rrpp-domain4] quit
```

Create RRPP ring group 1, and add subrings 2 and 3 in RRPP domains 1 and 2 to the RRPP ring group.

```
[DeviceD] rrpp ring 1
[DeviceD-ring-group1] domain 1 ring 2 3
[DeviceD-ring-group1] domain 2 ring 2 3
[DeviceD-ring-group1] quit
```

Enable RRPP.

```
[DeviceD] rrpp enable
```

Configuring Device E

Create VLANs 100 through 200.

```
<DeviceE> system-view
[DeviceE] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 1 vlan 100 to 150
[DeviceE-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceE] interface gigabitethernet 1/0/1
[DeviceE-GigabitEthernet1/0/1] undo shutdown
[DeviceE-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceE-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceE-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceE-GigabitEthernet1/0/1] link-delay up 0
[DeviceE-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceE-GigabitEthernet1/0/1] undo stp enable
[DeviceE-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceE] interface gigabitethernet 1/0/2
[DeviceE-GigabitEthernet1/0/2] undo shutdown
[DeviceE-GigabitEthernet1/0/2] port link-type trunk
[DeviceE-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceE-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet1/0/2] link-delay up 0
[DeviceE-GigabitEthernet1/0/2] link-delay down 0
[DeviceE-GigabitEthernet1/0/2] undo stp enable
[DeviceE-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceE] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceE-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 2.

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceE-rrpp-domain1] ring 2 enable
[DeviceE-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceE] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceE-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device E as the master node of subring 2, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 2.

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceE] rrpp enable
```

Configuring Device F

Create VLANs 100 through 200.

```
<DeviceF> system-view
[DeviceF] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 100 to 150
[DeviceF-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceF] interface gigabitethernet 1/0/1
[DeviceF-GigabitEthernet1/0/1] undo shutdown
[DeviceF-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceF-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceF-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceF-GigabitEthernet1/0/1] link-delay up 0
[DeviceF-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceF-GigabitEthernet1/0/1] undo stp enable
[DeviceF-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceF] interface gigabitethernet 1/0/2
[DeviceF-GigabitEthernet1/0/2] undo shutdown
[DeviceF-GigabitEthernet1/0/2] port link-type trunk
[DeviceF-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceF-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet1/0/2] link-delay up 0
[DeviceF-GigabitEthernet1/0/2] link-delay down 0
[DeviceF-GigabitEthernet1/0/2] undo stp enable
[DeviceF-GigabitEthernet1/0/2] quit
```

Create RRPP domain 1.

```
[DeviceF] rrpp domain 1
```

Configure VLAN 1000 as the primary control VLAN of RRPP domain 1.

```
[DeviceF-rrpp-domain1] control-vlan 1000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 1.

```
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
```

Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 3.

```
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

Create RRPP domain 2.

```
[DeviceF] rrpp domain 2
```

Configure VLAN 2000 as the primary control VLAN of RRPP domain 2.

```
[DeviceF-rrpp-domain2] control-vlan 2000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 2.

```
[DeviceF-rrpp-domain2] protected-vlan reference-instance 2
```

Configure Device F as the master node of subring 3, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 3.

```
[DeviceF-rrpp-domain2] ring 3 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 1
[DeviceF-rrpp-domain2] ring 3 enable
[DeviceF-rrpp-domain2] quit
```

Enable RRPP.

```
[DeviceF] rrpp enable
```

Configuring Device G

Create VLANs 100 through 200.

```
<DeviceG> system-view
[DeviceG] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceG] stp region-configuration
[DeviceG-mst-region] instance 1 vlan 100 to 150
[DeviceG-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceG-mst-region] active region-configuration
[DeviceG-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceG] interface gigabitethernet 1/0/1
[DeviceG-GigabitEthernet1/0/1] undo shutdown
[DeviceG-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceG-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceG-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceG-GigabitEthernet1/0/1] link-delay up 0
[DeviceG-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceG-GigabitEthernet1/0/1] undo stp enable
[DeviceG-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceG] interface gigabitethernet 1/0/2
[DeviceG-GigabitEthernet1/0/2] undo shutdown
[DeviceG-GigabitEthernet1/0/2] port link-type trunk
[DeviceG-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceG-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceG-GigabitEthernet1/0/2] link-delay up 0
[DeviceG-GigabitEthernet1/0/2] link-delay down 0
[DeviceG-GigabitEthernet1/0/2] undo stp enable
[DeviceG-GigabitEthernet1/0/2] quit
```

Create RRPP domain 3.

```
[DeviceG] rrpp domain 3
```

Configure VLAN 3000 as the primary control VLAN of RRPP domain 3.

```
[DeviceG-rrpp-domain3] control-vlan 3000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 3.

```
[DeviceG-rrpp-domain3] protected-vlan reference-instance 1
```

Configure Device G as the transit node of primary ring 4, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 4.

```
[DeviceG-rrpp-domain1] ring 4 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceG-rrpp-domain1] ring 4 enable
[DeviceG-rrpp-domain1] quit
```

Create RRPP domain 4.

```
[DeviceG] rrpp domain 4
```

Configure VLAN 4000 as the primary control VLAN of RRPP domain 4.

```
[DeviceG-rrpp-domain4] control-vlan 4000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 4.

```
[DeviceG-rrpp-domain4] protected-vlan reference-instance 2
```

Configure Device G as the transit node of primary ring 4, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 4.

```
[DeviceG-rrpp-domain4] ring 4 node-mode transit primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceG-rrpp-domain4] ring 4 enable
[DeviceG-rrpp-domain4] quit
```

Enable RRPP.

```
[DeviceG] rrpp enable
```

Configuring Device H

Create VLANs 100 through 200.

```
<DeviceH> system-view
[DeviceH] vlan 100 to 200
```

Map VLANs 100 through 150 to MSTI 1, and VLANs 151 through 200 to MSTI 2.

```
[DeviceH] stp region-configuration
```

```
[DeviceH-mst-region] instance 1 vlan 100 to 150
[DeviceH-mst-region] instance 2 vlan 151 to 200
```

Activate the MST region configuration.

```
[DeviceH-mst-region] active region-configuration
[DeviceH-mst-region] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port.

```
[DeviceH] interface gigabitethernet 1/0/1
[DeviceH-GigabitEthernet1/0/1] undo shutdown
[DeviceH-GigabitEthernet1/0/1] port link-type trunk
```

Assign the port to VLANs 100 through 200, and remove it from VLAN 1.

```
[DeviceH-GigabitEthernet1/0/1] port trunk permit vlan 100 to 200
[DeviceH-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Set the physical state change suppression interval to 0 seconds on the port.

```
[DeviceH-GigabitEthernet1/0/1] link-delay up 0
[DeviceH-GigabitEthernet1/0/1] link-delay down 0
```

Disable the spanning tree feature on the port.

```
[DeviceH-GigabitEthernet1/0/1] undo stp enable
[DeviceH-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 in the same way GigabitEthernet 1/0/1 is configured.

```
[DeviceH] interface gigabitethernet 1/0/2
[DeviceH-GigabitEthernet1/0/2] undo shutdown
[DeviceH-GigabitEthernet1/0/2] port link-type trunk
[DeviceH-GigabitEthernet1/0/2] port trunk permit vlan 100 to 200
[DeviceH-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceH-GigabitEthernet1/0/2] link-delay up 0
[DeviceH-GigabitEthernet1/0/2] link-delay down 0
[DeviceH-GigabitEthernet1/0/2] undo stp enable
[DeviceH-GigabitEthernet1/0/2] quit
```

Create RRPP domain 3.

```
[DeviceH] rrpp domain 3
```

Configure VLAN 3000 as the primary control VLAN of RRPP domain 3.

```
[DeviceH-rrpp-domain3] control-vlan 3000
```

Configure the VLANs mapped to MSTI 1 as the protected VLANs of RRPP domain 3.

```
[DeviceH-rrpp-domain3] protected-vlan reference-instance 1
```

Configure Device H as the master node of primary ring 4, with GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Enable ring 4.

```
[DeviceH-rrpp-domain3] ring 4 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[DeviceH-rrpp-domain3] ring 4 enable
[DeviceH-rrpp-domain3] quit
```

Create RRPP domain 4.

```
[DeviceH] rrpp domain 4
```

Configure VLAN 4000 as the primary control VLAN of RRPP domain 4.

```
[DeviceH-rrpp-domain4] control-vlan 4000
```

Configure the VLANs mapped to MSTI 2 as the protected VLANs of RRPP domain 4.

```
[DeviceH-rrpp-domain4] protected-vlan reference-instance 2
```

Configure Device H as the master node of primary ring 4, with GigabitEthernet 1/0/2 as the primary port and GigabitEthernet 1/0/1 as the secondary port. Enable ring 4.

```
[DeviceH-rrpp-domain4] ring 4 node-mode master primary-port gigabitethernet 1/0/2
secondary-port gigabitethernet 1/0/1 level 0
[DeviceH-rrpp-domain4] ring 4 enable
[DeviceH-rrpp-domain4] quit
```

Enable RRPP.

```
[DeviceH] rrpp enable
```

Verifying the configuration

View detailed information about RRPP domain 1 on Device A.

```
[DeviceA] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                  Port status: UP
 Secondary port: GE1/0/2                  Port status: BLOCKED
```

The output shows the following information:

- Device A is the master node of primary ring 1 in RRPP domain 1.
- The primary ring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device A.

```
[DeviceA] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
```

```
 Primary port  : GE1/0/1                  Port status: UP
 Secondary port: GE1/0/2                  Port status: UP
```

The output shows the following information:

- Device A is the transit node of primary ring 1 in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 1 on Device B.

```
[DeviceB] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                  Port status: UP
 Secondary port: GE1/0/1                  Port status: UP
```

The output shows the following information:

- Device B is the transit node of primary ring 1 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device B.

```
[DeviceB] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                  Port status: UP
 Secondary port: GE1/0/1                  Port status: BLOCKED
```

The output shows the following information:

- Device B is the master node of primary ring 1 in RRPP domain 2.
- The primary ring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 1 on Device C.

```
[DeviceC] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/4                   Port status: UP
```

The output shows the following information:

- Device C is the transit node of primary ring 1 and edge node of subrings 2 and 3 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device C.

```
[DeviceC] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
```

```
 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/4                   Port status: UP
```

The output shows the following information:

- Device C is the transit node of primary ring 1 and edge node of subrings 2 and 3 in RRPP domain 2.
- The primary and secondary ports are up.

View RRPP ring group information for the edge node and assistant edge node on Device C.

```
[DeviceC] display rrpp ring-group 1
Ring Group 1:
Domain 1 Ring 2 to 3
Domain 2 Ring 2 to 3
```

View detailed information about RRPP domain 1 on Device D.

```
[DeviceD] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
```

```
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/4                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 1 and assistant edge node of subrings 2 and 3 in RRPP domain 1.
- The primary and secondary ports are up.

View detailed information about RRPP domain 2 on Device D.

```
[DeviceD] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 1
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: UP

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
```

```
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/3                   Port status: UP

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Assistant-edge
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Common port   : GE1/0/1                   Port status: UP
                 GE1/0/2                   Port status: UP
 Edge port     : GE1/0/4                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 1 and assistant edge node of subrings 2 and 3 in RRPP domain 2.
- The primary and secondary ports are up.

View detailed information about RRPP domain 3 on Device D.

```
[DeviceD] display rrpp verbose domain 3
 Domain ID     : 3
 Control VLAN  : Primary 3000, Secondary 3001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/5                   Port status: UP
 Secondary port: GE1/0/6                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 4 in RRPP domain 3.
- The primary and secondary ports are up.

View detailed information about RRPP domain 4 on Device D.

```
[DeviceD] display rrpp verbose domain 4
 Domain ID     : 4
 Control VLAN  : Primary 4000, Secondary 4001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
```

```
 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/5                   Port status: UP
 Secondary port: GE1/0/6                   Port status: UP
```

The output shows the following information:

- Device D is the transit node of primary ring 4 in RRPP domain 4.
- The primary and secondary ports are up.

View RRPP ring group information for the edge node and assistant edge node on Device D.

```
[DeviceD] display rrpp ring-group 1
Ring Group 1:
Domain 1 Ring 2 to 3
Domain 2 Ring 2 to 3
```

View detailed information about RRPP domain 1 on Device E.

```
[DeviceE] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: BLOCKED
```

The output shows the following information:

- Device E is the master node of subring 2 in RRPP domain 1.
- The subring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device E.

```
[DeviceE] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
```

```
 Ring ID       : 2
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                   Port status: UP
 Secondary port: GE1/0/2                   Port status: BLOCKED
```

The output shows the following information:

- Device E is the master node of subring 2 in RRPP domain 2.
- The subring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 1 on Device F.

```
[DeviceF] display rrpp verbose domain 1
 Domain ID     : 1
 Control VLAN  : Primary 1000, Secondary 1001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: BLOCKED
```

The output shows the following information:

- Device F is the master node of subring 3 in RRPP domain 1.
- The subring state of RRPP domain 1 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 2 on Device F.

```
[DeviceF] display rrpp verbose domain 2
 Domain ID     : 2
 Control VLAN  : Primary 2000, Secondary 2001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 3
 Ring Level    : 1
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
```

```
 Primary port  : GE1/0/1                    Port status: UP
 Secondary port: GE1/0/2                    Port status: BLOCKED
```

The output shows the following information:

- Device F is the master node of subring 3 in RRPP domain 2.
- The subring state of RRPP domain 2 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 3 on Device H.

```
[DeviceH] display rrpp verbose domain 3
 Domain ID     : 3
 Control VLAN  : Primary 3000, Secondary 3001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/1                    Port status: UP
 Secondary port: GE1/0/2                    Port status: BLOCKED
```

The output shows the following information:

- Device H is the master node of primary ring 4 in RRPP domain 3.
- The primary ring state of RRPP domain 3 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 4 on Device H.

```
[DeviceH] display rrpp verbose domain 4
 Domain ID     : 4
 Control VLAN  : Primary 4000, Secondary 4001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Master
 Ring State    : Completed
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                    Port status: UP
 Secondary port: GE1/0/1                    Port status: BLOCKED
```

The output shows the following information:

- Device H is the master node of primary ring 4 in RRPP domain 4.

- The primary ring state of RRPP domain 4 is completed.
- The primary port is up, and the secondary port is blocked.

View detailed information about RRPP domain 3 on Device G.

```
[DeviceG] display rrpp verbose domain 3
 Domain ID     : 3
 Control VLAN  : Primary 3000, Secondary 3001
 Protected VLAN: Reference instance 1
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: UP
```

The output shows the following information:

- Device G is the transit node of primary ring 4 in RRPP domain 3.
- The primary and secondary ports are up.

View detailed information about RRPP domain 4 on Device G.

```
[DeviceG] display rrpp verbose domain 4
 Domain ID     : 4
 Control VLAN  : Primary 4000, Secondary 4001
 Protected VLAN: Reference instance 2
 Hello timer   : 1 seconds, Fail timer: 3 seconds
 Fast detection status: Disabled
 Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
 Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

 Ring ID       : 4
 Ring Level    : 0
 Node Mode     : Transit
 Ring State    : -
 Enable Status : Yes    Active Status: Yes
 Primary port  : GE1/0/2                   Port status: UP
 Secondary port: GE1/0/1                   Port status: UP
```

The output shows the following information:

- Device G is the transit node of primary ring 4 in RRPP domain 4.
- The primary and secondary ports are up.

Configuration files

NOTE:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
 sysname DeviceA
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device B:

```
#
 sysname DeviceB
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 1 enable
#
rrpp enable
#
```

- Device C:

```
#
```

```
 sysname DeviceC
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
```

```
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
 ring 3 node-mode edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode edge edge-port GigabitEthernet1/0/3
 ring 2 enable
 ring 3 node-mode edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
rrpp enable
#
```

- Device D:

```
#
 sysname DeviceD
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
```

```
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 1 enable
 ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
 ring 2 enable
 ring 3 node-mode assistant-edge edge-port GigabitEthernet1/0/4
 ring 3 enable
#
rrpp domain 3
 control-vlan 3000
 protected-vlan reference-instance 1
 ring 4 node-mode transit primary-port GigabitEthernet1/0/5 secondary-port
GigabitEthernet1/0/6 level 0
 ring 4 enable
#
rrpp domain 4
 control-vlan 4000
 protected-vlan reference-instance 2
 ring 4 node-mode transit primary-port GigabitEthernet1/0/5 secondary-port
GigabitEthernet1/0/6 level 0
 ring 4 enable
#
rrpp ring-group 1
 domain 1 ring 2 to 3
 domain 2 ring 2 to 3
#
rrpp enable
#
```

- Device E:

```
#
 sysname DeviceE
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
```

```
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 2 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
 ring 2 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 2 enable
#
rrpp enable
#
```

- Device F:

```
#
 sysname DeviceF
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 1
 control-vlan 1000
 protected-vlan reference-instance 1
 ring 3 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 1
 ring 3 enable
#
rrpp domain 2
 control-vlan 2000
 protected-vlan reference-instance 2
 ring 3 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 1
 ring 3 enable
#
rrpp enable
#
```

- Device G:

```
#
 sysname DeviceG
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 3
 control-vlan 3000
 protected-vlan reference-instance 1
 ring 4 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 4 enable
#
rrpp domain 4
 control-vlan 4000
 protected-vlan reference-instance 2
 ring 4 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 4 enable
#
rrpp enable
#
```

- Device H:

```
#
 sysname DeviceH
#
vlan 1
#
vlan 100 to 200
#
stp region-configuration
 instance 1 vlan 100 to 150
 instance 2 vlan 151 to 200
 active region-configuration
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 to 200
 link-delay up 0
 link-delay down 0
 undo stp enable
#
rrpp domain 3
 control-vlan 3000
 protected-vlan reference-instance 1
 ring 4 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
GigabitEthernet1/0/2 level 0
 ring 4 enable
#
rrpp domain 4
 control-vlan 4000
 protected-vlan reference-instance 2
 ring 4 node-mode master primary-port GigabitEthernet1/0/2 secondary-port
GigabitEthernet1/0/1 level 0
 ring 4 enable
#
rrpp enable
#
```

Contents

Introduction

This document provides examples for configuring BGP route selection based on route attributes.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

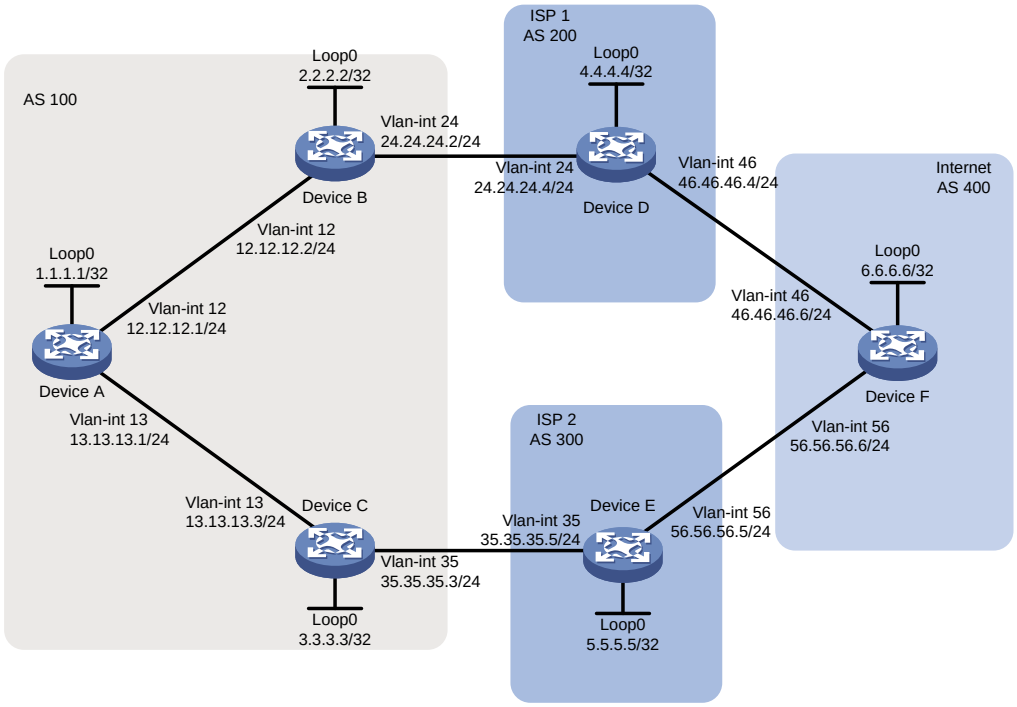
This document assumes that you have basic knowledge of BGP and routing policy.

Example: Configuring route selection based on the AS_PATH attribute

Network configuration

As shown in Figure 1, all devices run BGP. Configure a routing policy on Device B and Device C so that traffic from AS 100 to AS 400 is preferentially forwarded by Device D.

Figure 1 Network diagram



Analysis

For devices in AS 100 to select the optimal route based on AS numbers, increase the local preference for routes whose AS_PATH attributes end with the specified AS number. Configure a routing policy on Device C to set the local preference to 300 for routes whose AS_PATH attributes end with AS number 400.

To filter routes based on AS numbers, use an AS path list.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI	Release 63xx

Hardware	Software version
S5500V3-48P-SI	
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported

Hardware	Software version
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Procedures

Configuring IP addresses for interfaces

Configure an IP address for the interface VLAN-interface 12 on Device A.

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 12
[DeviceA-Vlan-interface12] ip address 12.12.12.1 24
[DeviceA-Vlan-interface12] quit
```

Configure IP addresses for other interfaces as shown in Figure 1. (Details not shown.)

Configuring BGP connections

On Device A, enable the default BGP instance, set the AS number to 100, and specify 12.12.12.2 and 13.13.13.3 as BGP peers.

```
[DeviceA] bgp 100
[DeviceA-bgp-default] router-id 1.1.1.1
[DeviceA-bgp-default] peer 12.12.12.2 as-number 100
[DeviceA-bgp-default] peer 13.13.13.3 as-number 100
[DeviceA-bgp-default] address-family ipv4 unicast
[DeviceA-bgp-default-ipv4] peer 12.12.12.2 enable
[DeviceA-bgp-default-ipv4] peer 13.13.13.3 enable
[DeviceA-bgp-default-ipv4] quit
[DeviceA-bgp-default] quit
```

On Device B, enable the default BGP instance, set the AS number to 100, specify 12.12.12.1 and 24.24.24.4 as BGP peers, and redistribute direct routes.

```
[DeviceB] bgp 100
[DeviceB-bgp-default] router-id 2.2.2.2
[DeviceB-bgp-default] peer 12.12.12.1 as-number 100
[DeviceB-bgp-default] peer 24.24.24.4 as-number 200
[DeviceB-bgp-default] address-family ipv4 unicast
[DeviceB-bgp-default-ipv4] peer 12.12.12.1 enable
[DeviceB-bgp-default-ipv4] peer 24.24.24.4 enable
[DeviceB-bgp-default-ipv4] import-route direct
[DeviceB-bgp-default-ipv4] quit
[DeviceB-bgp-default] quit
```

On Device C, enable the default BGP instance, set the AS number to 100, specify 13.13.13.1 and 35.35.35.5 as BGP peers, and redistribute direct routes.

```
[DeviceC] bgp 100
[DeviceC-bgp-default] router-id 3.3.3.3
[DeviceC-bgp-default] peer 13.13.13.1 as-number 100
[DeviceC-bgp-default] peer 35.35.35.5 as-number 300
[DeviceC-bgp-default] address-family ipv4 unicast
[DeviceC-bgp-default-ipv4] peer 13.13.13.1 enable
[DeviceC-bgp-default-ipv4] peer 35.35.35.5 enable
[DeviceC-bgp-default-ipv4] import-route direct
[DeviceC-bgp-default-ipv4] quit
[DeviceC-bgp-default] quit
```

On Device D, enable the default BGP instance, set the AS number to 200, specify 24.24.24.2 and 46.46.46.6 as BGP peers, and advertise the route 4.4.4.4/32.

```
[DeviceD] bgp 200
[DeviceD-bgp-default] router-id 4.4.4.4
[DeviceD-bgp-default] peer 24.24.24.2 as-number 100
[DeviceD-bgp-default] peer 46.46.46.6 as-number 400
[DeviceD-bgp-default] address-family ipv4 unicast
[DeviceD-bgp-default-ipv4] peer 24.24.24.2 enable
[DeviceD-bgp-default-ipv4] peer 46.46.46.6 enable
[DeviceD-bgp-default-ipv4] network 4.4.4.4 32
[DeviceD-bgp-default-ipv4] quit
[DeviceD-bgp-default] quit
```

On Device E, enable the default BGP instance, set the AS number to 300, specify 35.35.35.3 and 56.56.56.6 as BGP peers, and advertise the route 5.5.5.5/32.

```
[DeviceE] bgp 300
[DeviceE-bgp-default] router-id 5.5.5.5
[DeviceE-bgp-default] peer 35.35.35.3 as-number 100
[DeviceE-bgp-default] peer 56.56.56.6 as-number 400
[DeviceE-bgp-default] address-family ipv4 unicast
[DeviceE-bgp-default-ipv4] peer 35.35.35.3 enable
[DeviceE-bgp-default-ipv4] peer 56.56.56.6 enable
[DeviceE-bgp-default-ipv4] network 5.5.5.5 32
[DeviceE-bgp-default-ipv4] quit
[DeviceE-bgp-default] quit
```

On Device F, enable the default BGP instance, set the AS number to 400, specify 46.46.46.4 and 56.56.56.5 as BGP peers, and advertise the route 6.6.6.6/32.

```
[DeviceF] bgp 400
[DeviceF-bgp-default] router-id 6.6.6.6
[DeviceF-bgp-default] peer 46.46.46.4 as-number 200
[DeviceF-bgp-default] peer 56.56.56.5 as-number 300
[DeviceF-bgp-default] address-family ipv4 unicast
[DeviceF-bgp-default-ipv4] peer 46.46.46.4 enable
[DeviceF-bgp-default-ipv4] peer 56.56.56.5 enable
[DeviceF-bgp-default-ipv4] network 6.6.6.6 32
[DeviceF-bgp-default-ipv4] quit
[DeviceF-bgp-default] quit
```

Display the BGP routing table on Device A. The output shows the routes advertised by Device D, Device E, and Device F, and the AS_PATH attributes of the routes.

```
[DeviceA] display bgp routing-table ipv4

Total number of routes: 12

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 2.2.2.2/32         12.12.12.2      0          100        0       ?
* >i 3.3.3.3/32         13.13.13.3      0          100        0       ?
* >i 4.4.4.4/32         24.24.24.4      0          100        0       200i
*  i                    35.35.35.5                 100        0       300 400
                                                                      200i
* >i 5.5.5.5/32         35.35.35.5      0          100        0       300i
*  i                    24.24.24.4                 100        0       200 400
                                                                      300i
* >i 6.6.6.6/32         24.24.24.4                 100        0       200 400i
*  i                    35.35.35.5                 100        0       300 400i
* >i 12.12.12.0/24      12.12.12.2      0          100        0       ?
* >i 13.13.13.0/24      13.13.13.3      0          100        0       ?
* >i 24.24.24.0/24      12.12.12.2      0          100        0       ?
* >i 35.35.35.0/24      13.13.13.3      0          100        0       ?
```

Configuring routing policies

Create routing policy **aspath** on Device C, and set the local preference to 300 for routes whose AS_PATH attributes end with AS number 400.

```
[DeviceC] ip as-path 1 permit 400$
[DeviceC] route-policy aspath permit node 20
[DeviceC-route-policy-aspath-20] if-match as-path 1
[DeviceC-route-policy-aspath-20] apply local-preference 300
[DeviceC-route-policy-aspath-20] quit
[DeviceC] route-policy aspath permit node 25
```

Apply routing policy **aspath** to routes from the peer 35.35.35.5.

```
[DeviceC] bgp 100
[DeviceC-bgp-default] address-family ipv4
[DeviceC-bgp-default-ipv4] peer 35.35.35.5 route-policy aspath import
```

Verifying the configuration

Display the BGP routing table on Device A. The output shows that the next hop has changed for the route to AS 400.

```
[DeviceA] display bgp routing-table ipv4
```

```
Total number of routes: 11

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? – incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 2.2.2.2/32         12.12.12.2      0          100        0       ?
* >i 3.3.3.3/32         13.13.13.3      0          100        0       ?
* >i 4.4.4.4/32         24.24.24.4      0          100        0       200i
*  i                    35.35.35.5                 100        0       300 400
                                                                      200i
* >i 5.5.5.5/32         35.35.35.5      0          100        0       300i
*  i                    24.24.24.4                 100        0       200 400
                                                                      300i
* >i 6.6.6.6/32         35.35.35.5                 300        0       300 400i
*  i                    24.24.24.4                 100        0       200 400i
* >i 12.12.12.0/24      12.12.12.2      0          100        0       ?
* >i 13.13.13.0/24      13.13.13.3      0          100        0       ?
* >i 24.24.24.0/24      12.12.12.2      0          100        0       ?
* >i 35.35.35.0/24      13.13.13.3      0          100        0       ?
```

Verify that packets from Device A to 6.6.6.6 are forwarded by Device D.

```
[DeviceA] tracert 6.6.6.6
traceroute to 6.6.6.6 (6.6.6.6), 30 hops at most, 52 bytes each packet, press CT
RL+C to break
 1  12.12.12.2 (12.12.12.2)  2.417 ms  1.887 ms  1.773 ms
 2  35.35.35.5 (35.35.35.5)  4.057 ms  2.293 ms  2.739 ms
 3  6.6.6.6 (6.6.6.6)  5.145 ms  4.205 ms  4.402 ms
```

Configuration files

- Device A:

```
#
vlan 12
#
vlan 13
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
#
interface Vlan-interface13
 ip address 13.13.13.1 255.255.255.0
```

```
#
bgp 100
 router-id 1.1.1.1
 peer 12.12.12.2 as-number 100
 peer 13.13.13.3 as-number 100
 #
 address-family ipv4 unicast
  peer 12.12.12.2 enable
  peer 13.13.13.3 enable
#
```

- Device B:

```
#
vlan 12
#
vlan 24
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
#
interface Vlan-interface24
 ip address 24.24.24.2 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 12.12.12.1 as-number 100
 peer 24.24.24.4 as-number 200
 #
 address-family ipv4 unicast
  import-route direct
  peer 12.12.12.1 enable
  peer 24.24.24.4 enable
#
```

- Device C:

```
#
vlan 13
#
vlan 35
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface13
 ip address 13.13.13.3 255.255.255.0
#
interface Vlan-interface35
```

```
 ip address 35.35.35.3 255.255.255.0
#
bgp 100
 router-id 3.3.3.3
 peer 13.13.13.1 as-number 100
 peer 35.35.35.5 as-number 300
 #
 address-family ipv4 unicast
  import-route direct
  peer 13.13.13.1 enable
  peer 35.35.35.5 enable
  peer 35.35.35.5 route-policy aspath import
#
route-policy aspath permit node 20
 if-match as-path 1
 apply local-preference 300
route-policy aspath permit node 25
#
 ip as-path 1 permit 400$
#
```

- Device D:

```
#
vlan 24
#
vlan 46
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface24
 ip address 24.24.24.4 255.255.255.0
#
interface Vlan-interface46
 ip address 46.46.46.4 255.255.255.0
#
bgp 200
 router-id 4.4.4.4
 peer 24.24.24.2 as-number 100
 peer 46.46.46.6 as-number 400
 #
 address-family ipv4 unicast
  network 4.4.4.4 255.255.255.255
  peer 24.24.24.2 enable
  peer 46.46.46.6 enable
#
```

- Device E:

```
#
vlan 35
```

```
#
vlan 56
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
interface Vlan-interface35
 ip address 35.35.35.5 255.255.255.0
#
interface Vlan-interface56
 ip address 56.56.56.5 255.255.255.0
#
bgp 300
 router-id 5.5.5.5
 peer 35.35.35.3 as-number 100
 peer 56.56.56.6 as-number 400
 #
 address-family ipv4 unicast
  network 5.5.5.5 255.255.255.255
  peer 35.35.35.3 enable
  peer 56.56.56.6 enable
#
```

- Device F:

```
#
vlan 46
#
vlan 56
#
interface LoopBack0
 ip address 6.6.6.6 255.255.255.255
#
interface Vlan-interface46
 ip address 46.46.46.6 255.255.255.0
#
interface Vlan-interface56
 ip address 56.56.56.6 255.255.255.0
#
bgp 400
 router-id 6.6.6.6
 peer 46.46.46.4 as-number 200
 peer 56.56.56.5 as-number 300
 #
 address-family ipv4 unicast
  network 6.6.6.6 255.255.255.255
  peer 46.46.46.4 enable
  peer 56.56.56.5 enable
#
```

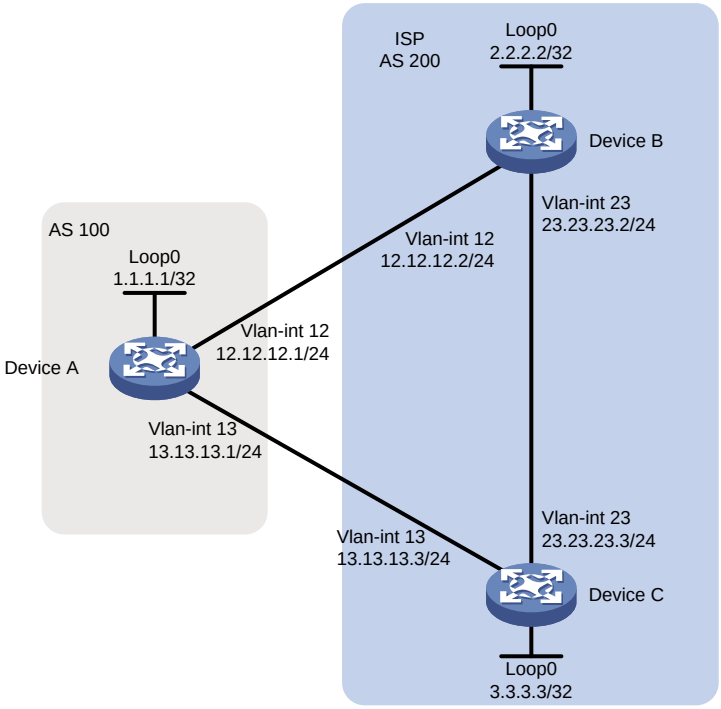
Example: Configuring route selection based on the MED attribute

Network configuration

As shown in Figure 2, all devices run BGP. EBGP runs between Device A and Device B, and between Device A and Device C. IBGP runs between Device B and Device C.

Configure a routing policy to ensure that traffic from AS 100 to AS 200 is preferentially forwarded by Device C. Before you configure the routing policy, the traffic is preferentially forwarded by Device B.

Figure 2 Network diagram



Analysis

To ensure that the traffic is preferentially forwarded by Device C, configure a routing policy on Device B to change the MED value for the route to Device A. Make sure the MED value is not the default MED value 0.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI	Release 11xx

Hardware	Software version
S5120V3-54P-PWR-SI	
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Procedures

Configuring basic BGP

Configure an IP address for the interface VLAN-interface 12 on Device A.

```
<DeviceA> system-view
```

```
[DeviceA] interface Vlan-interface 12
[DeviceA-Vlan-interface12] ip address 12.12.12.1 24
[DeviceA-Vlan-interface12] quit
```

Configure IP addresses for other interfaces as shown in Figure 2. (Details not shown.)

On Device A, enable the default BGP instance, set the AS number to 100, and specify 12.12.12.2 and 13.13.13.3 as BGP peers.

```
[DeviceA] bgp 100
[DeviceA-bgp-default] router-id 1.1.1.1
[DeviceA-bgp-default] peer 12.12.12.2 as-number 200
[DeviceA-bgp-default] peer 13.13.13.3 as-number 200
[DeviceA-bgp-default] address-family ipv4 unicast
[DeviceA-bgp-default-ipv4] peer 12.12.12.2 enable
[DeviceA-bgp-default-ipv4] peer 13.13.13.3 enable
[DeviceA-bgp-default-ipv4] quit
[DeviceA-bgp-default] quit
```

On Device B, enable the default BGP instance, set the AS number to 200, and specify 12.12.12.1 and 3.3.3.3 as BGP peers.

```
[DeviceB] bgp 200
[DeviceB-bgp-default] router-id 2.2.2.2
[DeviceB-bgp-default] peer 12.12.12.1 as-number 100
[DeviceB-bgp-default] peer 3.3.3.3 as-number 200
[DeviceB-bgp-default] peer 3.3.3.3 connect-interface LoopBack0
[DeviceB-bgp-default] address-family ipv4 unicast
[DeviceB-bgp-default-ipv4] peer 12.12.12.1 enable
[DeviceB-bgp-default-ipv4] peer 3.3.3.3 enable
[DeviceB-bgp-default-ipv4] network 23.23.23.0 24
[DeviceB-bgp-default-ipv4] quit
[DeviceB-bgp-default] quit
```

Configure a static route to 3.3.3.3/32 on Device B.

```
[DeviceB] ip route-static 3.3.3.3 32 23.23.23.3
```

On Device C, enable the default BGP instance, set the AS number to 200, and specify 13.13.13.1 and 2.2.2.2 as BGP peers.

```
[DeviceC] bgp 200
[DeviceC-bgp-default] router-id 3.3.3.3
[DeviceC-bgp-default] peer 13.13.13.1 as-number 100
[DeviceC-bgp-default] peer 2.2.2.2 as-number 200
[DeviceC-bgp-default] peer 2.2.2.2 connect-interface LoopBack0
[DeviceC-bgp-default] address-family ipv4 unicast
[DeviceC-bgp-default-ipv4] peer 13.13.13.1 enable
[DeviceC-bgp-default-ipv4] peer 2.2.2.2 enable
[DeviceC-bgp-default-ipv4] network 23.23.23.0 24
[DeviceC-bgp-default-ipv4] quit
[DeviceC-bgp-default] quit
```

Configure a static route to 2.2.2.2/32 on Device C.

```
[DeviceC] ip route-static 2.2.2.2 32 23.23.23.2
```

Display the BGP routing table on Device A. The output shows that the route with the next hop 12.12.12.2 becomes the optimal route to the network 23.23.23.0/24.

```
[DeviceA] display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 23.23.23.0/24      12.12.12.2      0                     0       200i
*  e                    13.13.13.3      0                     0       200i
```

Configuring a routing policy

Create routing policy 10 on Device B and set the cost to 100.

```
[DeviceB] route-policy 10 permit node 10
[DeviceB-route-policy-10-10] apply cost 100
[DeviceB-route-policy-10-10] quit
```

Apply routing policy 10 to routes to the peer 12.12.12.1.

```
[DeviceB] bgp 200
[DeviceB-bgp-default] address-family ipv4 unicast
[DeviceB-bgp-default-ipv4] peer 12.12.12.1 route-policy 10 export
[DeviceB-bgp-default-ipv4] quit
[DeviceB-bgp-default] quit
```

Verifying the configuration

Display the BGP routing table on Device A. The output shows that the MED value for the route with the next hop 12.12.12.2 changes to 100, and the route with the next hop 13.13.13.3 becomes the optimal route.

```
[DeviceA] display bgp routing-table ipv4

 Total number of routes: 2

 BGP local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e – external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 23.23.23.0/24      13.13.13.3      0                     0       200i
*  e                    12.12.12.2      100                   0       200i
```

Configuration files

- Device A:

```
#
vlan 12
#
vlan 13
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
#
interface Vlan-interface13
 ip address 13.13.13.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 peer 12.12.12.2 as-number 200
 peer 13.13.13.3 as-number 200
 #
 address-family ipv4 unicast
  peer 12.12.12.2 enable
  peer 13.13.13.3 enable
#
```

- Device B:

```
#
vlan 12
#
vlan 23
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
#
interface Vlan-interface23
 ip address 23.23.23.2 255.255.255.0
#
bgp 200
 router-id 2.2.2.2
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 peer 12.12.12.1 as-number 100
 #
 address-family ipv4 unicast
```

```
  network 23.23.23.0 255.255.255.0
  peer 3.3.3.3 enable
  peer 12.12.12.1 enable
  peer 12.12.12.1 route-policy 10 export
#
route-policy 10 permit node 10
 apply cost 100
#
 ip route-static 3.3.3.3 32 23.23.23.3
#
```

- Device C:

```
#
vlan 13
#
vlan 23
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface13
 ip address 13.13.13.3 255.255.255.0
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
#
bgp 200
 router-id 3.3.3.3
 peer 2.2.2.2 as-number 200
 peer 2.2.2.2 connect-interface LoopBack0
 peer 13.13.13.1 as-number 100
 #
 address-family ipv4 unicast
  network 23.23.23.0 255.255.255.0
  peer 2.2.2.2 enable
  peer 13.13.13.1 enable
#
 ip route-static 2.2.2.2 32 23.23.23.2
#
```

Contents

Introduction

This document provides IS-IS route summarization configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IS-IS route summarization.

Example: Configuring IS-IS route summarization

Network configuration

As shown in Figure 1, the five departments of a company use IS-IS to connect to the backbone network. The five departments are assigned the networks 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, and 192.168.5.0/24. Configure IS-IS route summarization to reduce routing entries and save system resources for Device B.

Figure 1 Network diagram

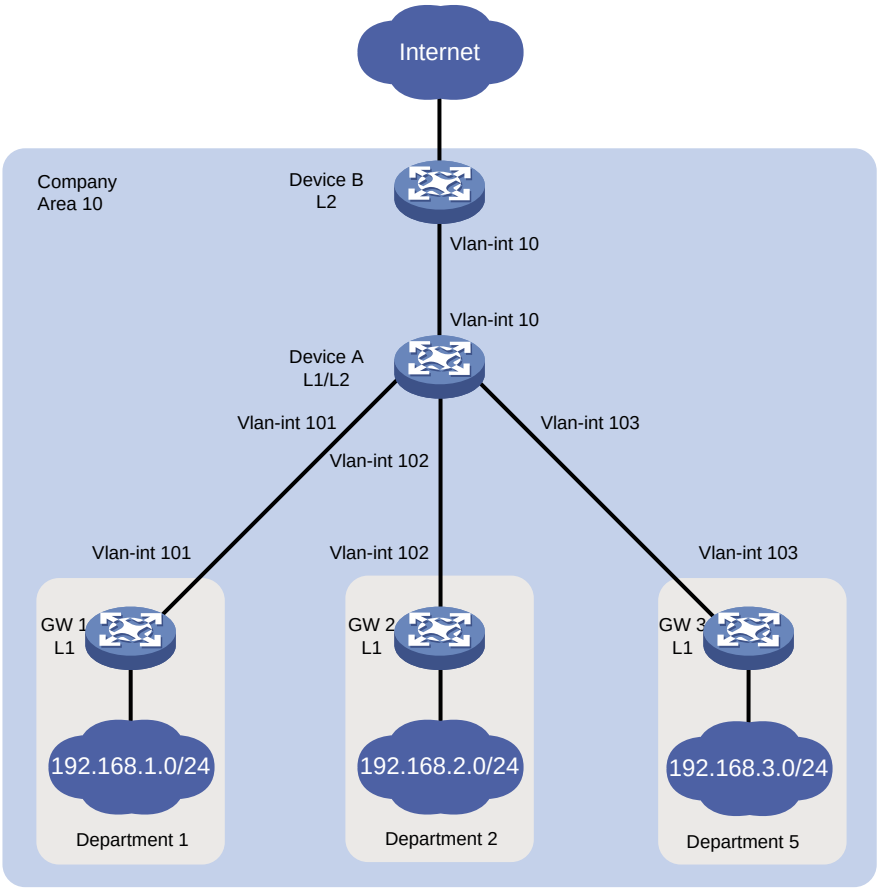


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int10	172.16.1.1/24	Device B	Vlan-int10	172.168.1.2/24
	Vlan-int101	10.1.1.1/24	GW 1	Vlan-int101	10.1.1.2/24
	Vlan-int102	10.1.2.1/24	GW 2	Vlan-int102	10.1.2.2/24
	Vlan-int103	10.1.3.1/24	GW3	Vlan-int103	10.1.3.2/24

Analysis

Configure route summarization on Device A because route summarization applies only to locally generated LSPs.

To avoid blackhole routes, set the summary route to 192.168.0.0/22.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Procedures

Configuring IP addresses for interfaces

Configure an IP address for the interface VLAN-interface 10 on Device A.

```
<DeviceA> system-view
```

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 172.16.1.1 24
[DeviceA-Vlan-interface10] quit
```

Configure IP addresses for other interfaces as shown in Figure 1 in the same way VLAN-interface 10 is configured. (Details not shown.)

Configuring basic IS-IS

Configuring Device A

Enable IS-IS on Device A and configure Device A as a Level-1-2 router.

```
[DeviceA] isis 1
[DeviceA-isis-1] network-entity 10.0000.0000.0001.00
[DeviceA-isis-1] is-level level-1-2
[DeviceA-isis-1] quit
```

Enable IS-IS on the interface VLAN-interface 10.

```
[DeviceA] interface vlan-interface 10
[DeviceA–Vlan-interface10] isis enable 1
[DeviceA–Vlan-interface10] quit
```

Configure other interfaces in the same way VLAN-interface 10 is configured. (Details not shown.)

Configuring Device B

Enable IS-IS on Device B and configure Device B as a Level-2 router.

```
[DeviceB] isis 1
[DeviceB-isis-1] network-entity 10.0000.0000.0002.00
[DeviceB-isis-1] is-level level-2
[DeviceB-isis-1] quit
```

Enable IS-IS on the interface VLAN-interface 10.

```
[DeviceB] interface vlan-interface 10
[DeviceB–Vlan-interface10] isis enable 1
[DeviceB–Vlan-interface10] quit
```

Configuring the gateways

Enable IS-IS on GW 1 and configure GW 1 as a Level-1 router.

```
[GW1] isis 1
[GW1-isis-1] network-entity 10.0001.0001.0001.00
[GW1-isis-1] is-level level-1
[GW1-isis-1] quit
```

Enable IS-IS on the interface VLAN-interface 11.

```
[GW1] interface vlan-interface 11
[GW1–Vlan-interface11] isis enable 1
[GW1–Vlan-interface11] quit
```

Configure other gateways in the same way GW 1 is configured. (Details not shown.)

Displaying IS-IS routing information on Device B

Display IS-IS routing information on Device B to view the network address of each department.

```
[DeviceB] display isis route

                    Route information for IS-IS(1)
```

```
                         ------------------------------

                         Level-2 IPv4 Forwarding Table
                         ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 192.168.1.0/24       30         NULL    Vlan10          172.16.1.1      R/-/-
 10.1.1.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 192.168.2.0/24       30         NULL    Vlan10          172.16.1.1      R/-/-
 10.1.2.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 192.168.3.0/24       30         NULL    Vlan10          172.16.1.1      R/-/-
 10.1.3.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 172.16.1.0/24        10         NULL    Vlan10          Direct          D/L/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

Configuring IS-IS route summarization

Configure IS-IS route summarization on Device A.

```
[DeviceA] isis 1
[DeviceA] address-family ipv4
[DeviceA-isis-1-ipv4]summary 192.168.0.0 22
```

Verifying the configuration

Display IS-IS routing information on Device B.

```
[DeviceB] display isis route

                         Route information for IS-IS(1)
                         ------------------------------

                         Level-2 IPv4 Forwarding Table
                         ------------------------------

 IPv4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
 10.1.1.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 10.1.2.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 10.1.3.0/24          20         NULL    Vlan10          172.16.1.1      R/-/-
 172.16.1.0/24        10         NULL    Vlan10          Direct          D/L/-
 192.168.0.0/22       30         NULL    Vlan10          172.16.1.1      R/-/-

      Flags: D-Direct, R-Added to Rib, L-Advertised in LSPs, U-Up/Down Bit Set
```

The output shows that the networks have been summarized into a single network 192.168.0.0/22.

Configuration files

- Device A:

```
#
isis 1
 network-entity 10.0000.0000.0001.00
 #
 address-family ipv4 unicast
  summary 192.168.0.0 255.255.252.0
#
vlan 10
#
vlan 101 to 103
#
interface vlan-interface10
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
interface vlan-interface101
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface vlan-interface102
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
#
interface vlan-interface103
 ip address 10.1.3.1 255.255.255.0
 isis enable 1
#
```

- Device B:

```
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
vlan 10
#
interface vlan-interface10
 ip address 172.16.1.2 255.255.255.0
 isis enable 1
#
```

- GW 1:

```
#
isis 1
 is-level level-1
 network-entity 10.0001.0001.0001.00
```

```
#
vlan 11
#
vlan 101
#
interface vlan-interface101
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
interface vlan-interface11
 ip address 192.168.1.1 255.255.255.0
 isis enable 1
#
```

- The configuration files for other gateways are similar to the configuration file for GW 1. (Details not shown.)

Contents

Introduction

This document provides Virtual eXtensible LAN (VXLAN) configuration examples. VXLAN is a MAC-in-UDP technology that provides Layer 2 connectivity between distant network sites across an IP network. VXLAN is typically used in data centers for multitenant services.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of VXLAN.

General restrictions and guidelines

As a best practice, do not configure multiple VXLAN tunnels to use the same source and destination IP addresses.

Link aggregation group membership is mutually exclusive with Ethernet service instance-to-VSI mappings on a Layer 2 interface. Do not map a VSI to an Ethernet service instance on a Layer 2 interface if the interface is in a Layer 2 aggregation group.

Ethernet service instance bindings of VSIs are mutually exclusive with QinQ and VLAN mapping on a Layer 2 Ethernet interface or Layer 2 aggregate interface. Do not configure these features simultaneously on the same interface. Otherwise, the features cannot take effect.

Do not configure VLAN mapping, QinQ, or MAC-based VLAN on a Layer 2 Ethernet interface or Layer 2 aggregate interface that acts as the outgoing interface for traffic of VXLAN tunnels. Otherwise, the features cannot take effect.

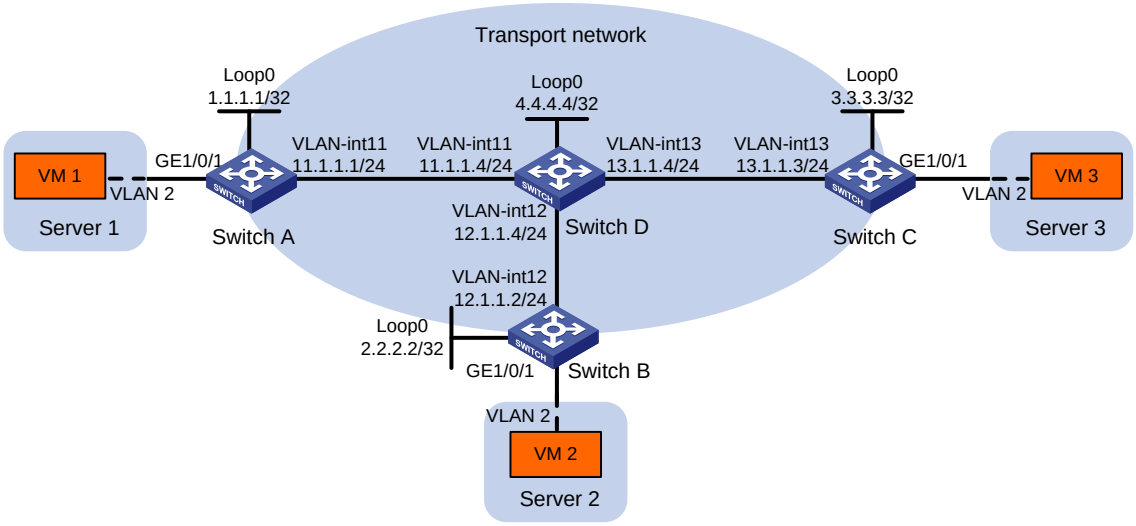
Example: Configuring VXLAN Layer 2 forwarding

Network configuration

As shown in Figure 1:

- Configure VXLAN 10 as a unicast-mode VXLAN on Switch A, Switch B, and Switch C to provide Layer 2 connectivity for the VMs across the network sites.
- Manually establish VXLAN tunnels and assign the tunnels to VXLAN 10.

Figure 1 Network diagram



Analysis

To ensure that the switches in the transport network can reach one another, configure a routing protocol on the switches to advertise routes for interfaces, including the loopback interfaces. In this example, OSPF is used.

To assign Switch A, Switch B, and Switch C to a VXLAN network, create VXLAN tunnels on the switches and assign the tunnels to the VXLAN.

To assign the customer traffic of a VLAN to a VXLAN, you must perform the following tasks:

- Create an Ethernet service instance on the interface that receives the traffic.
- Configure the Ethernet service instance to match the VLAN.
- Map the Ethernet service instance to the VSI on which the VXLAN is created.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported

Hardware	Software version
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

Execute the **undo vxlan ip-forwarding** command on each VTEP to enable Layer 2 forwarding for VXLANs on the VTEPs.

Procedures

Setting the system operation mode

Set the system operation mode to VXLAN on Switch A, Switch B, and Switch C. This step uses Switch A as an example. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
```

```
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Configuring IP addresses for interfaces

Configure IP addresses for interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 11
[SwitchA-vlan11] port gigabitethernet 1/0/2
[SwitchA-vlan11] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] quit
```

Configure IP addresses for interfaces on other switches in the same way the IP addresses are configured on Switch A. (Details not shown.)

Configuring a routing protocol on the transport network

Configure OSPF to advertise routes for Switch A.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure OSPF to advertise routes for Switch B.

```
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure OSPF to advertise routes for Switch C.

```
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure OSPF to advertise routes for Switch D.

```
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
```

```
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Configuring VXLAN settings

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
[SwitchA] undo vxlan ip-forwarding
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan10] quit
[SwitchA-vsi-vpna] quit
```

Create a VXLAN tunnel to Switch B. The tunnel interface name is **Tunnel 1**.

```
[SwitchA] interface tunnel 1 mode vxlan
[SwitchA-Tunnel1] source 1.1.1.1
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] quit
```

Create a VXLAN tunnel to Switch C. The tunnel interface name is **Tunnel 2**.

```
[SwitchA] interface tunnel 2 mode vxlan
[SwitchA-Tunnel2] source 1.1.1.1
[SwitchA-Tunnel2] destination 3.3.3.3
[SwitchA-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan10] tunnel 1
[SwitchA-vsi-vpna-vxlan10] tunnel 2
[SwitchA-vsi-vpna-vxlan10] quit
[SwitchA-vsi-vpna] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 1000 to match VLAN 2.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchA-GigabitEthernet1/0/1] service-instance 1000
[SwitchA-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchA-GigabitEthernet1/0/1-srv1000] quit
[SwitchA-GigabitEthernet1/0/1] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
[SwitchB] undo vxlan ip-forwarding
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan10] quit
[SwitchB-vsi-vpna] quit
```

Create a VXLAN tunnel to Switch A. The tunnel interface name is **Tunnel 1**.

```
[SwitchB] interface tunnel 1 mode vxlan
[SwitchB-Tunnel1] source 2.2.2.2
[SwitchB-Tunnel1] destination 1.1.1.1
[SwitchB-Tunnel1] quit
```

Create a VXLAN tunnel to Switch C. The tunnel interface name is **Tunnel 2**.

```
[SwitchB] interface tunnel 2 mode vxlan
[SwitchB-Tunnel2] source 2.2.2.2
[SwitchB-Tunnel2] destination 3.3.3.3
[SwitchB-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan10] tunnel 1
[SwitchB-vsi-vpna-vxlan10] tunnel 2
[SwitchB-vsi-vpna-vxlan10] quit
[SwitchB-vsi-vpna] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] service-instance 1000
[SwitchB-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchB-GigabitEthernet1/0/1-srv1000] quit
[SwitchB-GigabitEthernet1/0/1] quit
```

Configuring Switch C

Enable L2VPN.

```
[SwitchC] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
[SwitchC] undo vxlan ip-forwarding
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchC] vsi vpna
```

```
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan10] quit
[SwitchC-vsi-vpna] quit
```

Create a VXLAN tunnel to Switch A. The tunnel interface name is **Tunnel 1**.

```
[SwitchC] interface tunnel 1 mode vxlan
[SwitchC-Tunnel1] source 3.3.3.3
[SwitchC-Tunnel1] destination 1.1.1.1
[SwitchC-Tunnel1] quit
```

Create a VXLAN tunnel to Switch B. The tunnel interface name is **Tunnel 2**.

```
[SwitchC] interface tunnel 2 mode vxlan
[SwitchC-Tunnel2] source 3.3.3.3
[SwitchC-Tunnel2] destination 2.2.2.2
[SwitchC-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan10] tunnel 1
[SwitchC-vsi-vpna-vxlan10] tunnel 2
[SwitchC-vsi-vpna-vxlan10] quit
[SwitchC-vsi-vpna] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 1000 to match VLAN 2.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/1] service-instance 1000
[SwitchC-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchC-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchC-GigabitEthernet1/0/1-srv1000] quit
[SwitchC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

1. Verify the VXLAN settings on the VTEPs. This example uses Switch A.

   # Verify that the VXLAN tunnel interfaces on the VTEP are in up state.

   ```
   [SwitchA] display interface tunnel
   Tunnel1
   Current state: UP
   Line protocol state: UP
   Description: Tunnel1 Interface
   Bandwidth: 64 kbps
   Maximum transmission unit: 1464
   Internet protocol processing: Disabled
   Last clearing of counters: Never
   Tunnel source 1.1.1.1, destination 2.2.2.2
   Tunnel protocol/transport UDP_VXLAN/IP
   Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
   ```

```
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 3.3.3.3
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that the VXLAN tunnels have been assigned to the VXLAN, and the VXLAN tunnels and Ethernet service instances are in up state.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type        Flood proxy
    Tunnel1              0x5000001  Up     Manual      Disabled
    Tunnel2              0x5000002  Up     Manual      Disabled
  ACs:
    AC                              Link ID    State     Type
    GE1/0/1 srv1000                 0          Up        Manual
```

Verify that the VTEP has learned the MAC addresses of remote VMs.

```
[SwitchA] display l2vpn mac-address
MAC Address    State     VSI Name                        Link ID/Name   Aging
cc3e-5f9c-6cdb Dynamic   vpna                            Tunnel1        Aging
cc3e-5f9c-23dc Dynamic   vpna                            Tunnel2        Aging
```

```
--- 2 mac address(es) found  ---
```

2. Verify that VM 1, VM 2, and VM 3 can ping each other. (Details not shown.)

Configuration files

- Switch A:

```
#
 undo vxlan ip-forwarding ( Not applicable to S6550XE-HI and S6525XE-HI switch series.)
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 2
#
vlan 11
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
#
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 11
#
interface Tunnel1 mode vxlan
 source 1.1.1.1
 destination 2.2.2.2
#
```

```
interface Tunnel2 mode vxlan
 source 1.1.1.1
 destination 3.3.3.3
#
return
```

- Switch B:

```
#
 undo vxlan ip-forwarding
```
(Not applicable to S6550XE-HI and S6525XE-HI switch series.)
```
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.1.1.0 0.0.0.255
#
vlan 2
#
vlan 12
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
#
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface Tunnel1 mode vxlan
 source 2.2.2.2
 destination 1.1.1.1
#
```

```
interface Tunnel2 mode vxlan
 source 2.2.2.2
 destination 3.3.3.3
#
return
```

- Switch C:

```
#
 undo vxlan ip-forwarding
```
(Not applicable to S6550XE-HI and S6525XE-HI switch series.)
```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
vlan 2
#
vlan 13
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
#
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
interface Tunnel1 mode vxlan
 source 3.3.3.3
 destination 1.1.1.1
#
```

```
interface Tunnel2 mode vxlan
 source 3.3.3.3
 destination 2.2.2.2
#
return
```

- Switch D:

```
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 11.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 11
#
vlan 12
#
vlan 13
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.4 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.4 255.255.255.0
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
return
```

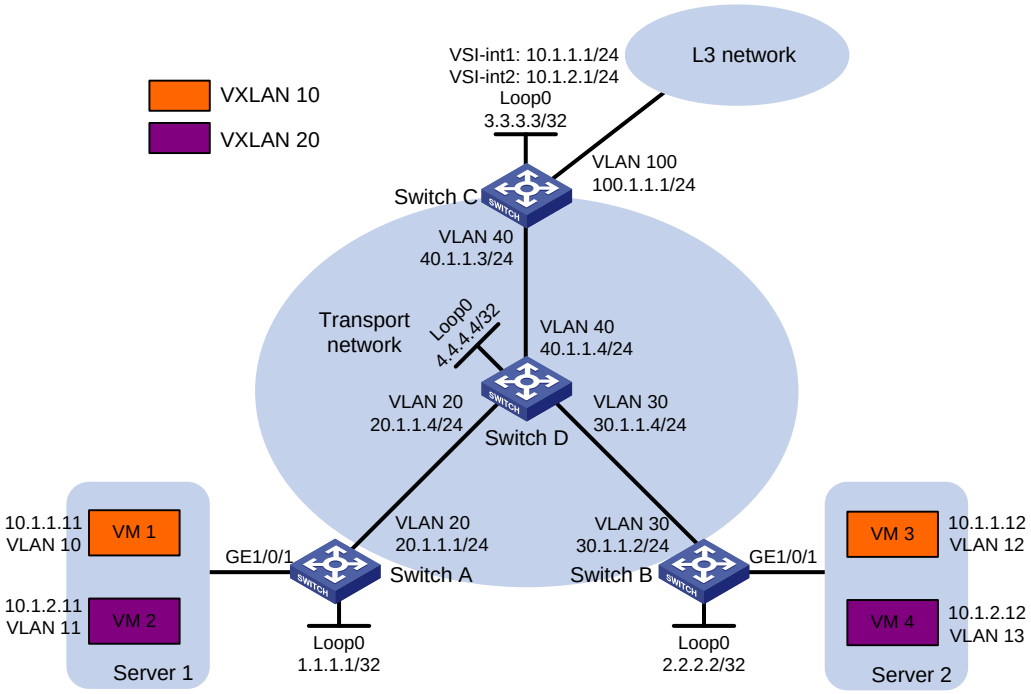
Example: Configuring a centralized VXLAN IP gateway

Network configuration

As shown in Figure 2:

- Configure VXLAN 10 and VXLAN 20 as unicast-mode VXLANs on Switch A, Switch B, and Switch C.
- Manually establish VXLAN tunnels and assign the tunnels to VXLAN 10 or VXLAN 20. Make sure VM 1 and VM 3 belong to VXLAN 10 and VM 2 and VM 4 belong to VXLAN 20.
- Configure a centralized VXLAN IP gateway on Switch C to provide gateway services for VXLAN 10 and VXLAN 20.

Figure 2 Network diagram



Analysis

To ensure that the switches in the transport network can reach one another, configure a routing protocol on the switches to advertise routes for interfaces, including the loopback interfaces. In this example, OSPF is used.

To assign Switch A, Switch B, and Switch C to VXLANs, create VXLAN tunnels on the switches and assign the tunnels to the VXLANs.

To assign the customer traffic of a VLAN to a VXLAN on Switch A or Switch B, you must perform the following tasks:

- Create an Ethernet service instance on the interface that receives the traffic.
- Configure the Ethernet service instance to match the VLAN.

- Map the Ethernet service instance to the VSI on which the VXLAN is created.

For Switch C to provide centralized VXLAN IP gateway services for VXLANs, you must perform the following tasks:

- Create a VSI interface for each VXLAN on the switch.
- Assign an IP address to each VSI interface.
- Specify the VSI interfaces as the gateway interfaces for VXLANs.

For Layer 3 nodes in the transport network to reach the VMs, configure a routing protocol on Switch C to advertise routes for VSI interfaces and VLAN-interface 100. In this example, OSPF is used.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported

Hardware	Software version
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported

Hardware	Software version
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Procedures

Setting the system operation mode

Set the system operation mode to VXLAN on Switch A, Switch B, and Switch C. This step uses Switch A as an example. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Configuring IP addresses for interfaces

Configure IP addresses for interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 20.1.1.1 24
[SwitchA-Vlan-interface20] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
```

Configure IP addresses for interfaces on other devices in the same way the IP addresses are configured on Switch A. (Details not shown.)

Configuring a routing protocol on the transport network

Configure OSPF to advertise routes for Switch A.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
```

```
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure OSPF to advertise routes for Switch B.

```
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure OSPF to advertise routes for Switch C.

```
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure OSPF to advertise routes for Switch D.

```
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Configuring basic VXLAN settings

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
[SwitchA] undo vxlan ip-forwarding
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan10] quit
[SwitchA-vsi-vpna] quit
```

Create VSI **vpnb** and VXLAN 20.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] vxlan 20
[SwitchA-vsi-vpnb-vxlan10] quit
[SwitchA-vsi-vpnb] quit
```

Create a VXLAN tunnel to Switch B. The tunnel interface name is **Tunnel 1**.

```
[SwitchA] interface tunnel 1 mode vxlan
[SwitchA-Tunnel1] source 1.1.1.1
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] quit
```

Create a VXLAN tunnel to Switch C. The tunnel interface name is **Tunnel 2**.

```
[SwitchA] interface tunnel 2 mode vxlan
[SwitchA-Tunnel2] source 1.1.1.1
[SwitchA-Tunnel2] destination 3.3.3.3
[SwitchA-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan10] tunnel 1
[SwitchA-vsi-vpna-vxlan10] tunnel 2
[SwitchA-vsi-vpna-vxlan10] quit
[SwitchA-vsi-vpna] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 20.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] vxlan 20
[SwitchA-vsi-vpnb-vxlan20] tunnel 1
[SwitchA-vsi-vpnb-vxlan20] tunnel 2
[SwitchA-vsi-vpnb-vxlan20] quit
[SwitchA-vsi-vpnb] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 1000 to match VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] service-instance 1000
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 10 11
[SwitchA-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 10
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchA-GigabitEthernet1/0/1-srv1000] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 2000 to match VLAN 11.

```
[SwitchA-GigabitEthernet1/0/1] service-instance 2000
[SwitchA-GigabitEthernet1/0/1-srv2000] encapsulation s-vid 11
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[SwitchA-GigabitEthernet1/0/1-srv2000] xconnect vsi vpnb
[SwitchA-GigabitEthernet1/0/1-srv2000] quit
[SwitchA-GigabitEthernet1/0/1] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs. This step is not applicable to S6550XE-HI and S6525XE-HI switch series.

```
[SwitchB] undo vxlan ip-forwarding
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan10] quit
[SwitchB-vsi-vpna] quit
```

Create VSI **vpnb** and VXLAN 20.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] vxlan 20
[SwitchB-vsi-vpnb-vxlan10] quit
[SwitchB-vsi-vpnb] quit
```

Create a VXLAN tunnel to Switch A. The tunnel interface name is **Tunnel 1**.

```
[SwitchB] interface tunnel 1 mode vxlan
[SwitchB-Tunnel1] source 2.2.2.2
[SwitchB-Tunnel1] destination 1.1.1.1
[SwitchB-Tunnel1] quit
```

Create a VXLAN tunnel to Switch C. The tunnel interface name is **Tunnel 2**.

```
[SwitchB] interface tunnel 2 mode vxlan
[SwitchB-Tunnel2] source 2.2.2.2
[SwitchB-Tunnel2] destination 3.3.3.3
[SwitchB-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan10] tunnel 1
[SwitchB-vsi-vpna-vxlan10] tunnel 2
[SwitchB-vsi-vpna-vxlan10] quit
[SwitchB-vsi-vpna] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 20.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] vxlan 20
[SwitchB-vsi-vpnb-vxlan20] tunnel 1
[SwitchB-vsi-vpnb-vxlan20] tunnel 2
[SwitchB-vsi-vpnb-vxlan20] quit
[SwitchB-vsi-vpnb] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 1000 to match VLAN 12.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 12 13
[SwitchB-GigabitEthernet1/0/1] service-instance 1000
[SwitchB-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 12
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchB-GigabitEthernet1/0/1-srv1000] quit
```

On GigabitEthernet 1/0/1, configure Ethernet service instance 2000 to match VLAN 13.

```
[SwitchB-GigabitEthernet1/0/1] service-instance 2000
[SwitchB-GigabitEthernet1/0/1-srv2000] encapsulation s-vid 13
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[SwitchB-GigabitEthernet1/0/1-srv2000] xconnect vsi vpnb
[SwitchB-GigabitEthernet1/0/1-srv2000] quit
[SwitchB-GigabitEthernet1/0/1] quit
```

Configuring Switch C

Enable L2VPN.

```
[SwitchC] l2vpn enable
```

Create VSI **vpna** and VXLAN 10.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan10] quit
[SwitchC-vsi-vpna] quit
```

Create VSI **vpnb** and VXLAN 20.

```
[SwitchC] vsi vpnb
[SwitchC-vsi-vpnb] vxlan 20
[SwitchC-vsi-vpnb-vxlan10] quit
[SwitchC-vsi-vpnb] quit
```

Create a VXLAN tunnel to Switch A. The tunnel interface name is **Tunnel 1**.

```
[SwitchC] interface tunnel 1 mode vxlan
[SwitchC-Tunnel1] source 3.3.3.3
[SwitchC-Tunnel1] destination 1.1.1.1
[SwitchC-Tunnel1] quit
```

Create a VXLAN tunnel to Switch B. The tunnel interface name is **Tunnel 2**.

```
[SwitchC] interface tunnel 2 mode vxlan
[SwitchC-Tunnel2] source 3.3.3.3
[SwitchC-Tunnel2] destination 2.2.2.2
[SwitchC-Tunnel2] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 10.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan10] tunnel 1
[SwitchC-vsi-vpna-vxlan10] tunnel 2
[SwitchC-vsi-vpna-vxlan10] quit
[SwitchC-vsi-vpna] quit
```

Assign Tunnel 1 and Tunnel 2 to VXLAN 20.

```
[SwitchC] vsi vpnb
[SwitchC-vsi-vpnb] vxlan 20
[SwitchC-vsi-vpnb-vxlan20] tunnel 1
[SwitchC-vsi-vpnb-vxlan20] tunnel 2
[SwitchC-vsi-vpnb-vxlan20] quit
[SwitchC-vsi-vpnb] quit
```

Configuring the centralized VXLAN IP gateway

Create VSI-interface 1 and assign the interface an IP address. The IP address will be used as the gateway address for VXLAN 10.

```
[SwitchC] interface vsi-interface 1
[SwitchC-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
```

```
[SwitchC-Vsi-interface1] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] gateway vsi-interface 1
[SwitchC-vsi-vpna] quit
```

Create VSI-interface 2 and assign the interface an IP address. The IP address will be used as the gateway address for VXLAN 20.

```
[SwitchC] interface vsi-interface 2
[SwitchC-Vsi-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchC-Vsi-interface2] quit
```

Specify VSI-interface 2 as the gateway interface for VSI **vpnb**.

```
[SwitchC] vsi vpnb
[SwitchC-vsi-vpnb] gateway vsi-interface 2
[SwitchC-vsi-vpnb] quit
```

Configure OSPF to advertise routes for the VSI interfaces and VLAN-interface 100.

```
[SwitchC] ospf 2 router-id 3.3.3.3
[SwitchC-ospf-2] area 0
[SwitchC-ospf-2-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-2-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchC-ospf-2-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[SwitchC-ospf-2-area-0.0.0.0] quit
[SwitchC-ospf-2] quit
```

Verifying the configuration

1. Verify the VXLAN settings on the VTEPs. This example uses Switch A.

Verify that the VXLAN tunnel interfaces are in up state.

```
[SwitchA] display interface tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
```

```
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 3.3.3.3
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that the VXLAN tunnels have been assigned to their respective VXLANs, and the VXLAN tunnels and Ethernet service instances are in up state.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State  Type        Flood proxy
    Tunnel1              0x5000001  Up     Manual      Disabled
    Tunnel2              0x5000002  Up     Manual      Disabled
  ACs:
    AC                               Link ID    State       Type
    GE1/0/1 srv1000                  0          Up          Manual

VSI Name: vpnb
  VSI Index               : 1
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
```

```
  Statistics              : Disabled
  VXLAN ID                : 20
  Tunnels:
    Tunnel Name           Link ID    State  Type        Flood proxy
    Tunnel1               0x5000001  Up     Manual      Disabled
    Tunnel2               0x5000002  Up     Manual      Disabled
  ACs:
    AC                                Link ID    State       Type
    GE1/0/1 srv2000                   0          Up          Manual
```

2. Verify the configuration on the VXLAN IP gateway:

Verify that the VXLAN tunnel interfaces are in up state.

```
[SwitchC] display interface tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 3.3.3.3, destination 1.1.1.1
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel2
Current state: UP
Line protocol state: UP
Description: Tunnel2 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 3.3.3.3, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that the VSI interfaces are in up state.

```
[SwitchC] display interface vsi-interface
Vsi-interface1
Current state: UP
Line protocol state: UP
Description: Vsi-interface1 Interface
Bandwidth: 1000000 kbps
```

```
Maximum transmission unit: 1500
Internet Address: 10.1.1.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0000-fc00-458d
IPv6 packet frame type: Ethernet II, hardware address: 0000-fc00-458d
Physical: Unknown, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Vsi-interface2
Current state: UP
Line protocol state: UP
Description: Vsi-interface2 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet Address:  10.1.2.1/24 (primary)
IP packet frame type: Ethernet II, hardware address: 0000-fc00-458d
IPv6 packet frame type: Ethernet II, hardware address: 0000-fc00-458d
Physical: Unknown, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that the VXLAN tunnels have been assigned to VXLANs 10 and 20, VSI-interface 1 is the gateway interface of VSI **vpna**, and VSI-interface 2 is the gateway interface of VSI **vpnb**.

```
[SwitchC] display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway interface       : VSI-interface 1
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flooding proxy
    Tunnel1              0x5000002  Up       Manual      Disabled
    Tunnel2              0x5000003  Up       Manual      Disabled
```

```
VSI Name: vpnb
  VSI Index               : 1
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway interface       : VSI-interface 2
  VXLAN ID                : 20
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flooding proxy
    Tunnel1              0x5000002  Up       Manual      Disabled
    Tunnel2              0x5000003  Up       Manual      Disabled
```

Verify that Switch C has created ARP entries for the VMs.

```
[SwitchC] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
10.1.1.11        0000-1234-0001 vpna         Tunnel1                 20    D
10.1.1.12        0000-1234-0002 vpna         Tunnel2                 19    D
```

Verify that Switch C has created FIB entries for the VMs.

```
[SwitchC] display fib 10.1.1.11

Destination count: 1 FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay     F:FRR

Destination/Mask   Nexthop         Flag     OutInterface/Token       Label
10.1.1.11/32       10.1.1.11       UH       Vsi1                     Null
```

3. Verify the network connectivity for VMs:

Verify that VM 1, VM 2, VM 3, and VM 4 can ping each other. (Details not shown.)

Verify that VM 1, VM 2, VM 3, VM 4, and VLAN-interface 100 (100.1.1.1) on Switch C can ping each other. (Details not shown.)

Configuration files

- Switch A:

  #

  `undo vxlan ip-forwarding` (Not applicable to S6550XE-HI and S6525XE-HI switch series.)

```
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 20.1.1.0 0.0.0.255
#
vlan 10
#
vlan 11
#
vlan 20
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
  tunnel 2
#
vsi vpnb
 vxlan 20
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 to 11
#
 service-instance 1000
  encapsulation s-vid 10
  xconnect vsi vpna
#
 service-instance 2000
  encapsulation s-vid 11
  xconnect vsi vpnb
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface Tunnel1 mode vxlan
```

```
 source 1.1.1.1
 destination 2.2.2.2
#
interface Tunnel2 mode vxlan
 source 1.1.1.1
 destination 3.3.3.3
```

- Switch B:

```
#
 undo vxlan ip-forwarding
```
(Not applicable to S6550XE-HI and S6525XE-HI switch series.)
```
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 30.1.1.0 0.0.0.255
#
vlan 12
#
vlan 13
#
vlan 30
#
 l2vpn enable
#
vsi vpna
 vxlan 10
  tunnel 1
  tunnel 2
#
vsi vpnb
 vxlan 20
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface30
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 12 to 13
#
 service-instance 1000
  encapsulation s-vid 12
  xconnect vsi vpna
#
```

```
 service-instance 2000
  encapsulation s-vid 13
  xconnect vsi vpnb
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface Tunnel1 mode vxlan
 source 2.2.2.2
 destination 1.1.1.1
#
interface Tunnel2 mode vxlan
 source 2.2.2.2
 destination 3.3.3.3
```

- Switch C:

```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 40.1.1.0 0.0.0.255
#
ospf 2 router-id 3.3.3.3
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
vlan 40
#
vlan 100
#
 l2vpn enable
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
  tunnel 1
  tunnel 2
#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
  tunnel 1
  tunnel 2
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
```

```
#
interface Vlan-interface40
 ip address 40.1.1.3 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
interface Vsi-interface1
 ip address 10.1.1.1 255.255.255.0
#
interface Vsi-interface2
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel1 mode vxlan
 source 3.3.3.3
 destination 1.1.1.1
#
interface Tunnel2 mode vxlan
 source 3.3.3.3
 destination 2.2.2.2
#
return
```

- Switch D:

```
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
vlan 20
#
vlan 30
#
vlan 40
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
```

```
interface Vlan-interface20
 ip address 20.1.1.4 255.255.255.0
#
interface Vlan-interface30
 ip address 30.1.1.4 255.255.255.0
#
interface Vlan-interface40
 ip address 40.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 40
#
return
```

Contents

Introduction

This document provides DRNI configuration examples.

Distributed Resilient Network Interconnect (DRNI) virtualizes two physical devices into one system through multichassis link aggregation. The standard for DRNI is IEEE P802.1AX-REV™/D4.4c, *Draft Standard for Local and Metropolitan Area Networks.*

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of DRNI.

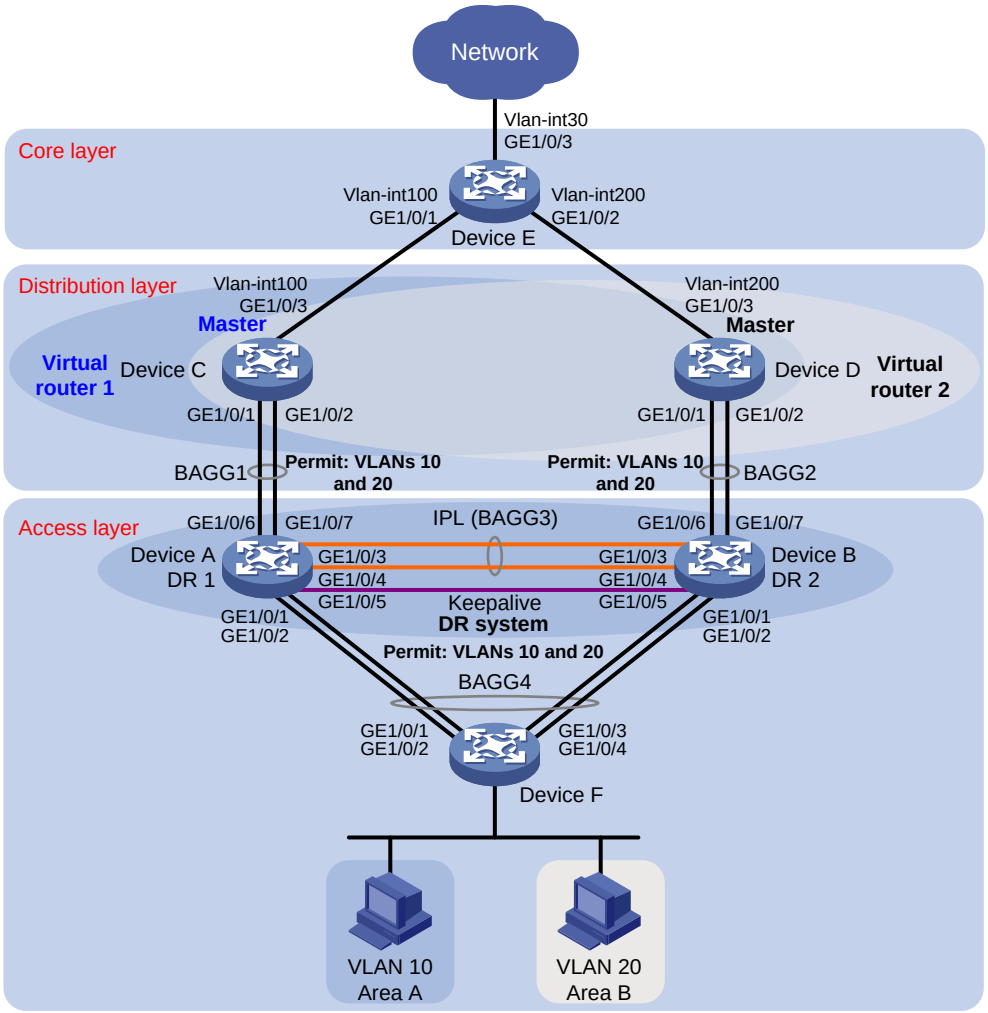
Example: Configuring DRNI at the access Layer

Network configuration

As shown in Figure 1:

- Configure Device A and Device B as a DR system to establish one multichassis aggregate link with Device F and one with Device C and Device D.
- Set up a keepalive link between GigabitEthernet 1/0/5 of Device A and GigabitEthernet 1/0/5 of Device B, and exclude the interfaces from the shutdown action by DRNI MAD.
- Configure two VRRP groups on Device C and Device D to provide gateway services for VLAN 10 and VLAN 20.
  - Configure VRRP group 1 to provide gateway services for hosts in VLAN 10 (Area A). Add Device C and Device D to the group as the master and backup devices, respectively.
  - Configure VRRP group 2 to provide gateway services for hosts in VLAN 20 (Area B). Add Device D and Device C to the group as the master and backup devices, respectively.
- Configure OSPF on Device C, Device D, and Device E for the hosts to communicate with external networks at Layer 3.

Figure 1 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	GE 1/0/5	1.1.1.1/24	Device B	GE1/0/5	1.1.1.2/24
Device C	VLAN-interface 100	100.1.1.1/24	Device D	VLAN-interface 100	200.1.1.1/24
	VLAN-interface 10	10.1.1.1/24		VLAN-interface 10	10.1.1.2/24
	VLAN-interface 20	20.1.1.1/24		VLAN-interface 20	20.1.1.2/24
	Virtual IP 1	10.1.1.100/24		Virtual IP 1	10.1.1.100/24
	Virtual IP 2	20.1.1.100/24		Virtual IP 2	20.1.1.100/24
Device E	VLAN-interface 100	100.1.1.2/24			
	VLAN-interface 200	200.1.1.2/24			
	VLAN-interface 30	30.1.1.1/24			

Analysis

For the secondary DR device to monitor the state of the primary device, establish a Layer 3 keepalive link between the DR member devices.

To balance traffic between two VRRP gateway devices, you can assign them to two VRRP groups with different priorities. In this example, Device C is assigned a higher priority than Device D in VRRP

group 1 so Device C can become the master in this group. Device D is assigned a higher priority than Device C in VRRP group 2 so Device D can become the master in this group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later
S6525XE-HI switch series	Release 6008 and later
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series	Not supported

Hardware	Software version
S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported

Hardware	Software version
S5135S-EI switch series	Not supported

Restrictions and guidelines

DRNI restrictions and guidelines

For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address and DR system priority on them. You must assign different DR system numbers to the DR member devices.

A DR member device can have only one IPP.

For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD.

VRRP restrictions and guidelines

You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.
- Invalid IP address (for example, 0.0.0.1).

The virtual IP address of an IPv4 VRRP group must be on the same subnet as the downlink interface IP addresses of the VRRP group members to ensure successful traffic forwarding.

Interface restrictions and guidelines

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **reserve-vlan-interface** command to reserve local VLAN interface resources. For more information about the reserve-vlan-interface command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause DR system setup failure.
Continue? [Y/N]:y
[DeviceA] drni system-number 1
Changing the system number might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[DeviceA] drni system-priority 123
```

```
Changing the system priority might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
```

Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface gigabitethernet 1/0/5
```

Create VLAN 10 and VLAN 20.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/6 and GigabitEthernet 1/0/7 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/6] quit
[DeviceA] interface gigabitethernet 1/0/7
[DeviceA-GigabitEthernet1/0/7] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/7] quit
```

Set the link type of Bridge-Aggregation 1 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceA-Bridge-Aggregation1] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3 and specify it as the IPP.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/3] quit
```

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/4] quit
```

Set the link type of Bridge-Aggregation 3 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port link-type trunk
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceA-Bridge-Aggregation3] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceA-Bridge-Aggregation3] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4 and assign it to DR group 4.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation4] port drni group 4
[DeviceA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 4.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 4
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 4
[DeviceA-GigabitEthernet1/0/2] quit
```

Set the link type of Bridge-Aggregation 4 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation4] quit
```

Configuring Device B

Configure DR system settings.

```
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause DR system setup failure.
Continue? [Y/N]:y
[DeviceB] drni system-number 2
Changing the system number might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[DeviceB] drni system-priority 123
Changing the system priority might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
```

Configure DR keepalive packet parameters.

```
[DeviceB] drni keepalive ip destination 1.1.1.1 source 1.1.1.2
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface gigabitethernet 1/0/5
```

Create VLAN 10 and VLAN 20.

```
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 2.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/6 and GigabitEthernet 1/0/7 to aggregation group 2.

```
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/6] quit
[DeviceB] interface gigabitethernet 1/0/7
[DeviceB-GigabitEthernet1/0/7] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/7] quit
```

Set the link type of Bridge-Aggregation 2 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] port link-type trunk
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceB-Bridge-Aggregation2] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceB-Bridge-Aggregation2] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3 and specify it as the IPP.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/4] quit
```

Set the link type of Bridge-Aggregation 3 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port link-type trunk
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceB-Bridge-Aggregation3] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceB-Bridge-Aggregation3] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4 and assign it to DR group 4.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation4] port drni group 4
[DeviceB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 4.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 4
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 4
[DeviceB-GigabitEthernet1/0/2] quit
```

Set the link type of Bridge-Aggregation 4 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation4] quit
```

Configuring Device C

Create VLAN 10, VLAN 20, and VLAN 100.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
[DeviceC] vlan 100
```

Assign GigabitEthernet 1/0/3 to VLAN 100.

```
[DeviceC] vlan 100
[DeviceC-vlan100] port gigabitethernet 1/0/3
[DeviceC-vlan100] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] link-aggregation mode dynamic
```

```
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet1/0/2 to aggregation group 1.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 1
[DeviceC-if-range] quit
```

Set the link type of Bridge-Aggregation 1 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation1] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation1] quit
```

Create uplink interface VLAN-interface 100 and assign it an IP address.

```
[DeviceC] interface vlan-interface 100
[DeviceC-Vlan-interface100] ip address 100.1.1.1 24
[DeviceC-Vlan-interface100] quit
```

Create VLAN-interface 10 and VLAN-interface 20 and assign an IP address to each of them.

```
[DeviceC] interface vlan-interface 10
[DeviceC-vlan-interface10] ip address 10.1.1.1 24
[DeviceC-vlan-interface10] quit
[DeviceC] interface vlan-interface 20
[DeviceC-vlan-interface20] ip address 20.1.1.1 24
[DeviceC-vlan-interface20] quit
```

Create VRRP group 1 on VLAN-interface 10 and set its virtual IP address to 10.1.1.100.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 virtual-ip 10.1.1.100
```

Set the priority of Device C to 200 for it to become the master in VRRP group 1.

```
[DeviceC-Vlan-interface10] vrrp vrid 1 priority 200
[DeviceC-Vlan-interface10] quit
```

Create VRRP group 2 on VLAN-interface 20 and set its virtual IP address to 20.1.1.100.

```
[DeviceC] interface vlan-interface 20
[DeviceC-Vlan-interface20] vrrp vrid 2 virtual-ip 20.1.1.100
[DeviceC-vlan-interface20] quit
```

Configure Device C to operate in preemptive mode in VRRP group 1. Set the preemption delay to 500 centiseconds to avoid frequent status switchover.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 preempt-mode delay 500
[DeviceC-Vlan-interface10] quit
```

Create track entry 1 to monitor the upstream link status of GigabitEthernet 1/0/3.

```
[DeviceC] track 1 interface gigabitethernet 1/0/3
```

Configure Device C in VRRP group 1 to monitor track entry 1, and decrease its priority by 150 when the track entry transits to Negative.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 track 1 priority reduced 150
```

```
[DeviceC-Vlan-interface10] quit
```

Configure OSPF.

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

Configuring Device D

Create VLAN 10, VLAN 20, and VLAN 200.

```
<DeviceD> system-view
[DeviceD] vlan 10
[DeviceD-vlan10] quit
[DeviceD] vlan 20
[DeviceD-vlan20] quit
[DeviceD] vlan 200
```

Assign GigabitEthernet 1/0/3 to VLAN 200.

```
[DeviceD] vlan 200
[DeviceD-vlan200] port gigabitethernet 1/0/3
[DeviceD-vlan200] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 2.

```
[DeviceD] interface bridge-aggregation 2
[DeviceD-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 2.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-aggregation group 2
[DeviceD-if-range] quit
```

Set the link type of Bridge-Aggregation 2 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceD] interface bridge-aggregation 2
[DeviceD-Bridge-Aggregation2] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation2] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation2] quit
```

Create uplink interface VLAN-interface 200 and assign it an IP address.

```
[DeviceD] interface vlan-interface 200
[DeviceD-Vlan-interface200] ip address 200.1.1.1 24
[DeviceD-Vlan-interface200] quit
```

Create VLAN-interface 10 and VLAN-interface 20 and assign an IP address to each of them.

```
[DeviceD] interface vlan-interface 10
[DeviceD-vlan-interface10] ip address 10.1.1.2 24
```

```
[DeviceD-vlan-interface10] quit
[DeviceD] interface vlan-interface 20
[DeviceD-vlan-interface20] ip address 20.1.1.2 24
[DeviceD-vlan-interface20] quit
```

Create VRRP group 1 on VLAN-interface 10 and set its virtual IP address to 10.1.1.100.

```
[DeviceD] interface vlan-interface 10
[DeviceD-Vlan-interface10] vrrp vrid 1 virtual-ip 10.1.1.100
[DeviceD-vlan-interface10] quit
```

Create VRRP group 2 on VLAN-interface 20 and set its virtual IP address to 20.1.1.100.

```
[DeviceD] interface vlan-interface 20
[DeviceD-Vlan-interface20] vrrp vrid 2 virtual-ip 20.1.1.100
```

Set the priority of Device D to 200 for it to become the master in VRRP group 2.

```
[DeviceD-Vlan-interface20] vrrp vrid 2 priority 200
```

Configure Device D to operate in preemptive mode in VRRP group 2. Set the preemption delay to 500 centiseconds to avoid frequent status switchover.

```
[DeviceD-Vlan-interface20] vrrp vrid 2 preempt-mode delay 500
[DeviceD-Vlan-interface20] quit
```

Create track entry 2 to monitor the upstream link status of GigabitEthernet 1/0/3.

```
[DeviceD] track 2 interface gigabitethernet 1/0/3
```

Configure Device D in VRRP group 2 to monitor track entry 2, and decrease its priority by 150 when the track entry transits to Negative.

```
[DeviceD] interface vlan-interface 20
[DeviceD-Vlan-interface20] vrrp vrid 2 track 2 priority reduced 150
[DeviceD-Vlan-interface20] quit
```

Configure OSPF.

```
[DeviceD] ospf
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Configuring Device E

Create VLAN 100 and assign GigabitEthernet 1/0/1 to the VLAN.

```
<DeviceE> system-view
[DeviceE] vlan 100
[DeviceE-vlan100] port gigabitethernet 1/0/1
[DeviceE-vlan100] quit
```

Create VLAN-interface 100 and assign it an IP address.

```
[DeviceE] interface vlan-interface 100
[DeviceE-vlan-interface100] ip address 100.1.1.2 24
[DeviceE-vlan-interface100] quit
```

Create VLAN 200 and assign GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceE] vlan 200
[DeviceE-vlan200] port gigabitethernet 1/0/2
```

```
[DeviceE-vlan200] quit
```

Create VLAN-interface 200 and assign it an IP address.

```
[DeviceE] interface vlan-interface 200
[DeviceE-vlan-interface200] ip address 200.1.1.2 24
[DeviceE-vlan-interface200] quit
```

Create VLAN 30 and assign GigabitEthernet 1/0/3 to the VLAN.

```
[DeviceE] vlan 30
[DeviceE-vlan30] port gigabitethernet 1/0/3
[DeviceE-vlan30] quit
```

Create VLAN-interface 30 and assign it an IP address.

```
[DeviceE] interface vlan-interface 30
[DeviceE-vlan-interface30] ip address 30.1.1.1 24
[DeviceE-vlan-interface30] quit
```

Configure OSPF.

```
[DeviceD] ospf
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Configuring Device F

Create VLAN 10 and VLAN 20.

```
[DeviceF] vlan 10
[DeviceF-vlan10] quit
[DeviceF] vlan 20
[DeviceF-vlan20] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[DeviceF] interface bridge-aggregation 4
[DeviceF-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceF-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to aggregation group 4.

```
[DeviceF] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceF-if-range] port link-aggregation group 4
[DeviceF-if-range] quit
```

Set the link type of Bridge-Aggregation 4 to trunk and assign it to VLAN 10 and VLAN 20.

```
[DeviceF] interface bridge-aggregation 4
[DeviceF-Bridge-Aggregation4] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceF-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
```

```
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceF-Bridge-Aggregation4] quit
```

Verifying the configuration

This configuration example uses the output from Release 6615P03. The command output varies by software version.

Verify that Device A and Device B have formed a DR system.

```
[DeviceA] display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG3
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time (s)
BAGG4         4         UP                   UP          -
[DeviceA] display drni verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired

IPP/IPP ID: BAGG3/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (260), GE1/0/4 (261)
Peer Selected ports indexes: 260, 261

DR interface/DR group ID: BAGG4/4
Local DR interface state: UP
Peer DR interface state: UP
DR group state: UP
Local DR interface down cause: -
Remaining DRNI DOWN time: -
Local DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local DR interface LACP priority: Config=123, Effective=123
Peer DR interface LACP priority: Config=123, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (258), GE1/0/2 (259)
Peer Selected ports indexes: 258, 259
```

Verify that all member ports of aggregation group 4 are in Selected state on Device F, which indicates a successful link aggregation between the DR system and Device F.

```
[DeviceF] display link-aggregation verbose
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation4
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 1eba-3c46-0300
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
  GE1/0/3             S        32768    3        1                      {ACDEF}
  GE1/0/4             S        32768    4        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16385    40004    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    16388    40004    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/3             32768    32769    40004    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/4             32768    32772    40004    0x7b  , 0001-0001-0001 {ACDEF}
```

Verify that Device C is the master in VRRP group 1 and Device D is the master in VRRP group 2.

```
[DeviceC] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan10             1     Master       200     100     None     10.1.1.100
 Vlan20             2     Backup       100     100     None     20.1.1.100
[DeviceD] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan10             1     Backup       100     100     None     10.1.1.100
 Vlan20             2     Master       200     100     None     20.1.1.100
```

Verify that Device E has established OSPF neighbor relationships with Device C and Device D.

```
[DeviceE] display ospf peer

         OSPF Process 1 with Router ID 200.1.1.2
```

```
              Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 100.1.1.1       100.1.1.1       1   35         Full/BDR          Vlan100
 200.1.1.1       200.1.1.1       1   33         Full/BDR          Vlan200
```

Verify that the host in Area A can ping VLAN-interface 30 (30.1.1.1) on Device E.

```
C:\Documents and Settings\Administrator>ping 30.1.1.1

Pinging 30.1.1.1 with 32 bytes of data:

Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 30.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
 port drni group 4
```

```
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 3
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 123
 drni keepalive ip destination 1.1.1.2 source 1.1.1.1
#
 drni mad exclude interface GigabitEthernet1/0/5
#
```

- Device B:

```
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
 port drni group 4
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 1 10 20
 port link-aggregation group 3
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 123
 drni keepalive ip destination 1.1.1.1 source 1.1.1.2
#
 drni mad exclude interface GigabitEthernet1/0/5
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 100
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.100
 vrrp vrid 1 priority 200
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 150
#
```

```
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
 vrrp vrid 2 virtual-ip 20.1.1.100
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
 track 1 interface GigabitEthernet1/0/3
#
```

- Device D:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 200
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.100
#
```

```
interface Vlan-interface20
 ip address 20.1.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 20.1.1.100
 vrrp vrid 2 priority 200
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 2 priority reduced 150
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 200
#
 track 2 interface GigabitEthernet1/0/3
#
```

- Device E:

```
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
#
vlan 30
#
vlan 100
#
vlan 200
#
interface Vlan-interface30
 ip address 30.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
#
```

```
interface Vlan-interface200
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
```

- Device F:

```
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
```

```
 port link-aggregation group 4
#
```

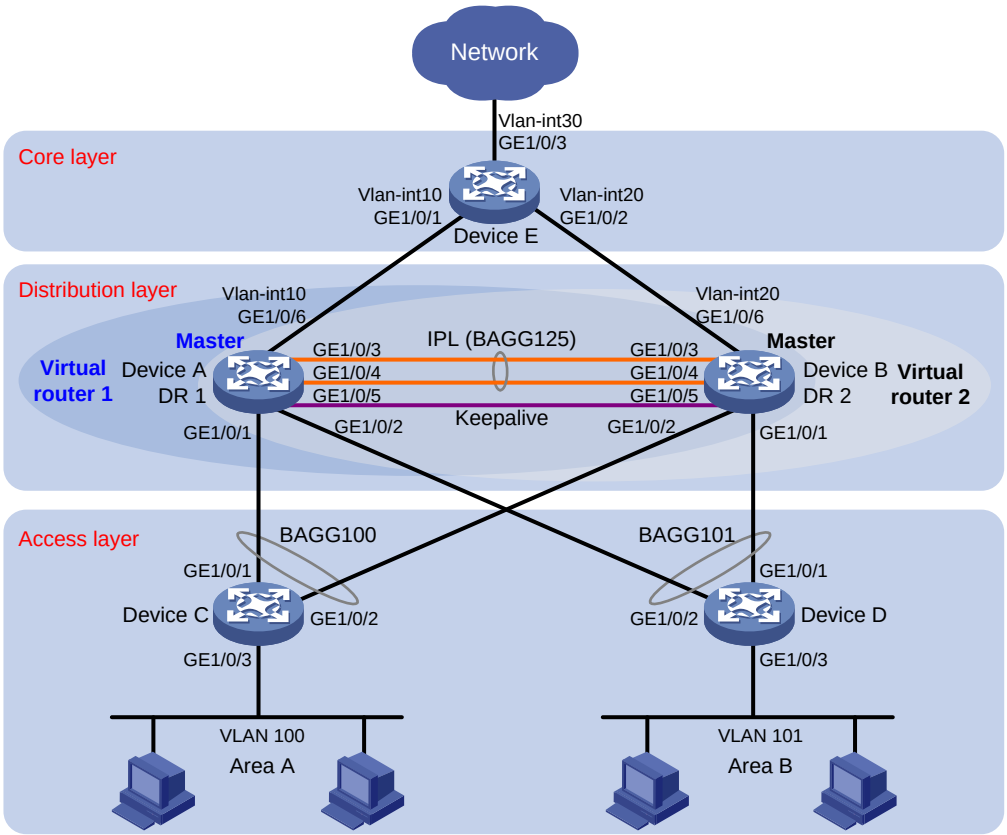
Example: Configuring DRNI at the distribution Layer

Network configuration

As shown in Figure 2:

- Configure Device A and Device B as a DR system to establish one multichassis aggregate link with Device C and Device D.
- Set up a keepalive link between GigabitEthernet 1/0/5 of Device A and GigabitEthernet 1/0/5 of Device B, and exclude the interfaces from the shutdown action by DRNI MAD.
- Configure two VRRP groups on Device A and Device B to provide gateway services for VLAN 100 and VLAN 101.
  - Configure VRRP group 1 to provide gateway services for hosts in VLAN 100 (Area A). Add Device A and Device B to the group as the master and backup devices, respectively.
  - Configure VRRP group 2 to provide gateway services for hosts in VLAN 101 (Area B). Add Device B and Device A to the group as the master and backup devices, respectively.
- Configure OSPF on Device A, Device B, and Device E for the hosts to communicate with external networks at Layer 3.

Figure 2 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	GE 1/0/5	1.1.1.1/24	Device B	GE 1/0/5	1.1.1.2/24
	VLAN-interface 100	100.1.1.1/24		VLAN-interface 100	100.1.1.2/24
	VLAN-interface 101	101.1.1.1/24		VLAN-interface 101	101.1.1.2/24
	VLAN-interface 10	10.1.1.1/24		VLAN-interface 20	20.1.1.1/24
	Virtual IP 1	100.1.1.100/24		Virtual IP 1	100.1.1.100/24
	Virtual IP 2	101.1.1.100/24		Virtual IP 2	101.1.1.100/24
Device E	VLAN-interface 10	10.1.1.2/24			
	VLAN-interface 20	20.1.1.2/24			
	VLAN-interface 30	30.1.1.1/24			

Analysis

For the secondary DR device to monitor the state of the primary device, establish a Layer 3 keepalive link between the DR member devices.

For Device A to be the master in VRRP group 1, assign it a higher priority than Device B. For Device B to be the master in VRRP group 2, assign it a higher priority than Device A.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx
S6550XE-HI switch series	Release 6008 and later
S6525XE-HI switch series	Release 6008 and later
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx,

Hardware	Software version
	Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series	Not supported

Hardware	Software version
MS4300V2 switch series MS4320 switch series MS4200 switch series	
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

DRNI restrictions and guidelines

For the DR member devices to be identified as one DR system, you must configure the same DR system MAC address and DR system priority on them. You must assign different DR system numbers to the DR member devices.

To balance traffic between two VRRP gateway devices, you can assign them to two VRRP groups with different priorities. In this example, Device A is assigned a higher priority than Device B in VRRP group 1 so Device A can become the master in this group. Device B is assigned a higher priority than Device A in VRRP group 2 so Device B can become the master in this group.

A DR member device can have only one IPP.

For correct keepalive detection, you must exclude the interfaces used for keepalive detection from the shutdown action by DRNI MAD.

VRRP restrictions and guidelines

You cannot specify the virtual IP address as any of the following IP addresses:

- All-zero address (0.0.0.0).
- Broadcast address (255.255.255.255).
- Loopback address.
- IP address of other than Class A, Class B, and Class C.
- Invalid IP address (for example, 0.0.0.1).

The virtual IP address of an IPv4 VRRP group must be on the same subnet as the downlink interface IP addresses of the VRRP group members to ensure successful traffic forwarding.

Interface restrictions and guidelines

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **reserve-vlan-interface** command to reserve local VLAN interface resources. For more information about the reserve-vlan-interface command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause DR system setup failure.
Continue? [Y/N]:y
[DeviceA] drni system-number 1
Changing the system number might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[DeviceA] drni system-priority 123
Changing the system priority might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
```

Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ip destination 1.1.1.2 source 1.1.1.1
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface gigabitethernet 1/0/5
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125 and specify it as the IPP.

```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation125] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation125] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 125.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceA-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100 and assign it to DR group 1.

```
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation100] port drni group 1
[DeviceA-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 100.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 100
[DeviceA-GigabitEthernet1/0/1] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101 and assign it to DR group 2.

```
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation101] port drni group 2
[DeviceA-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 101
[DeviceA-GigabitEthernet1/0/2] quit
```

Create VLAN 10, VLAN 100, and VLAN 101.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit
```

Assign GigabitEthernet 1/0/6 to VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/6
[DeviceA-vlan10] quit
```

Set the link type of Bridge-Aggregation 100 to trunk and assign it to VLAN 100.

```
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
[DeviceA-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/1 done.
[DeviceA-Bridge-Aggregation100] quit
```

Set the link type of Bridge-Aggregation 101 to trunk and assign it to VLAN 101.

```
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation101] quit
```

Set the link type of Bridge-Aggregation 125 to trunk and assign it to VLAN 100 and VLAN 101.

```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] port link-type trunk
Configuring GigabitEthernet1/0/3 done.
```

```
Configuring GigabitEthernet1/0/4 done.
[DeviceA-Bridge-Aggregation125] port trunk permit vlan 100 101
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceA-Bridge-Aggregation125] quit
```

Create VLAN-interface 10, VLAN-interface 100, and VLAN-interface 101 and assign an IP address to each of them.

```
[DeviceA] interface vlan-interface 10
[DeviceA-vlan-interface10] ip address 10.1.1.1 24
[DeviceA-vlan-interface10] quit
[DeviceA] interface vlan-interface 100
[DeviceA-vlan-interface100] ip address 100.1.1.1 24
[DeviceA-vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-vlan-interface101] ip address 101.1.1.1 24
[DeviceA-vlan-interface101] quit
```

Configure OSPF.

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 101.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 100.1.1.100.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 virtual-ip 100.1.1.100
```

Set the priority of Device A to 200 for it to become the master in VRRP group 1.

```
[DeviceA-Vlan-interface100] vrrp vrid 1 priority 200
[DeviceA-Vlan-interface100] quit
```

Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 101.1.1.100.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 2 virtual-ip 101.1.1.100
[DeviceA-Vlan-interface101] quit
```

Configure Device A to operate in preemptive mode in VRRP group 1. Set the preemption delay to 500 centiseconds to avoid frequent status switchover.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface100] quit
```

Create track entry 1 to monitor the upstream link status of GigabitEthernet 1/0/6.

```
[DeviceA] track 1 interface gigabitethernet 1/0/6
```

Configure Device A in VRRP group 1 to monitor track entry 1, and decrease its priority by 150 when the track entry transits to Negative.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 track 1 priority reduced 150
[DeviceA-Vlan-interface100] quit
```

Configuring Device B

Configure DR system settings.

```
<DeviceB> system-view
[DeviceB] drni system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause DR system setup failure.
Continue? [Y/N]:y
[DeviceB] drni system-number 2
Changing the system number might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
[DeviceB] drni system-priority 123
Changing the system priority might flap the intra-portal link and cause DR system setup
failure. Continue? [Y/N]:y
```

Configure DR keepalive packet parameters.

```
[DeviceB] drni keepalive ip destination 1.1.1.1 source 1.1.1.2
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface gigabitethernet 1/0/5
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 125 and specify it as the IPP.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation125] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation125] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 125.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceB-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100 and assign it to DR group 1.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation100] port drni group 1
[DeviceB-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 100.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 100
[DeviceB-GigabitEthernet1/0/2] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101 and assign it to DR group 2.

```
[DeviceB] interface bridge-aggregation 101
```

```
[DeviceB-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation101] port drni group 2
[DeviceB-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 101.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 101
[DeviceB-GigabitEthernet1/0/1] quit
```

Create VLAN 20, VLAN 100, and VLAN 101.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] vlan 101
[DeviceB-vlan101] quit
```

Assign GigabitEthernet 1/0/6 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/6
[DeviceB-vlan20] quit
```

Set the link type of Bridge-Aggregation 100 to trunk and assign it to VLAN 100.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation100] quit
```

Set the link type of Bridge-Aggregation 101 to trunk and assign it to VLAN 101.

```
[DeviceB] interface bridge-aggregation 101
[DeviceB-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
[DeviceB-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/1 done.
[DeviceB-Bridge-Aggregation101] quit
```

Set the link type of Bridge-Aggregation 125 to trunk and assign it to VLAN 100 and VLAN 101.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] port link-type trunk
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceB-Bridge-Aggregation125] port trunk permit vlan 100 101
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceB-Bridge-Aggregation125] quit
```

Create VLAN-interface 20, VLAN-interface 100, and VLAN-interface 101 and assign an IP address to each of them.

```
[DeviceB] interface vlan-interface 20
[DeviceB-vlan-interface20] ip address 20.1.1.1 24
[DeviceB-vlan-interface20] quit
[DeviceB] interface vlan-interface 100
```

```
[DeviceB-vlan-interface100] ip address 100.1.1.2 24
[DeviceB-vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ip address 101.1.1.2 24
[DeviceB-vlan-interface101] quit
```

Configure OSPF.

```
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 101.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 100.1.1.100.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] vrrp vrid 1 virtual-ip 100.1.1.100
[DeviceB-Vlan-interface100] quit
```

Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 101.1.1.100.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 2 virtual-ip 101.1.1.100
```

Set the priority of Device B to 200 for it to become the master in VRRP group 2.

```
[DeviceB-Vlan-interface101] vrrp vrid 2 priority 200
```

Configure Device B to operate in preemptive mode in VRRP group 2. Set the preemption delay to 500 centiseconds to avoid frequent status switchover.

```
[DeviceB-Vlan-interface101] vrrp vrid 2 preempt-mode delay 500
[DeviceB-Vlan-interface101] quit
```

Create track entry 2 to monitor the upstream link status of GigabitEthernet 1/0/6.

```
[DeviceB] track 2 interface gigabitethernet 1/0/6
```

Configure Device B in VRRP group 2 to monitor track entry 2, and decrease its priority by 150 when the track entry transits to Negative.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 2 track 2 priority reduced 150
[DeviceB-Vlan-interface101] quit
```

Configuring Device C

Create VLAN 100.

```
[DeviceC] vlan 100
[DeviceC-vlan100] quit
```

Assign GigabitEthernet 1/0/3 to VLAN 100.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 100
[DeviceC-GigabitEthernet1/0/3] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 100.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] link-aggregation mode dynamic
```

```
[DeviceC-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 100.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 100
[DeviceC-if-range] quit
```

Set the link type of Bridge-Aggregation 100 to trunk and assign it to VLAN 100.

```
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation100] quit
```

Configuring Device D

Create VLAN 101.

```
[DeviceD] vlan 101
[DeviceD-vlan101] quit
```

Assign GigabitEthernet 1/0/3 to VLAN 101.

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] port access vlan 101
[DeviceD-GigabitEthernet1/0/3] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 101.

```
<DeviceD> system-view
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-aggregation group 101
[DeviceD-if-range] quit
```

Set the link type of Bridge-Aggregation 101 to trunk and assign it to VLAN 101.

```
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation101] quit
```

Configuring Device E

Create VLAN 10 and assign GigabitEthernet 1/0/1 to the VLAN.

```
<DeviceE> system-view
```

```
[DeviceE] vlan 10
[DeviceE-vlan10] port gigabitethernet 1/0/1
[DeviceE-vlan10] quit
```

Create VLAN-interface 10 and assign it an IP address.

```
[DeviceE] interface vlan-interface 10
[DeviceE-vlan-interface10] ip address 10.1.1.2 24
[DeviceE-vlan-interface10] quit
```

Create VLAN 20 and assign GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceE] vlan 20
[DeviceE-vlan20] port gigabitethernet 1/0/2
[DeviceE-vlan20] quit
```

Create VLAN-interface 20 and assign it an IP address.

```
[DeviceE] interface vlan-interface 20
[DeviceE-vlan-interface20] ip address 20.1.1.2 24
[DeviceE-vlan-interface20] quit
```

Create VLAN 30 and assign GigabitEthernet 1/0/3 to the VLAN.

```
[DeviceE] vlan 30
[DeviceE-vlan30] port gigabitethernet 1/0/3
[DeviceE-vlan30] quit
```

Create VLAN-interface 30 and assign it an IP address.

```
[DeviceE] interface vlan-interface 30
[DeviceE-vlan-interface30] ip address 30.1.1.1 24
[DeviceE-vlan-interface30] quit
```

Configure OSPF.

```
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

Verifying the configuration

This configuration example uses the output from Release 6615P03. The command output varies by software version.

Verify that Device A and Device B have formed a DR system.

```
[DeviceA] display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG125
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time (s)
```

```
BAGG100       1         UP                  UP          -
BAGG101       2         UP                  UP          -
[DeviceA] display drni verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired

IPP/IPP ID: BAGG125/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (261), GE1/0/4 (262)
Peer Selected ports indexes: 261, 262

DR interface/DR group ID: BAGG100/1
Local DR interface state: UP
Peer DR interface state: UP
DR group state: UP
Local DR interface down cause: -
Remaining DRNI DOWN time: -
Local DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local DR interface LACP priority: Config=123, Effective=123
Peer DR interface LACP priority: Config=123, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (259)
Peer Selected ports indexes: 259

DR interface/DR group ID: BAGG101/2
Local DR interface state: UP
Peer DR interface state: UP
DR group state: UP
Local DR interface down cause: -
Remaining DRNI DOWN time: -
Local DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer DR interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local DR interface LACP priority: Config=123, Effective=123
Peer DR interface LACP priority: Config=123, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/2 (260)
Peer Selected ports indexes: 260
```

Verify that all member ports of aggregation group 100 are in Selected state on Device C, which indicates a successful link aggregation between the DR system and Device C.

```
[DeviceC] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
```

```
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation100
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 8e33-8e4a-0300
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16386    40001    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    32770    40001    0x7b  , 0001-0001-0001 {ACDEF}
```

Verify that all member ports of aggregation group 101 are in Selected state on Device D, which indicates a successful link aggregation between the DR system and Device D.

```
[DeviceD] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation101
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 8e33-9400-0400
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16387    40002    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    32771    40002    0x7b  , 0001-0001-0001 {ACDEF}
```

Verify that Device A is the master in VRRP group 1 and Device B is the master in VRRP group 2.

```
[DeviceA] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
```

```
 ------------------------------------------------------------------------
 Vlan100            1     Master       200     100     None     100.1.1.100
 Vlan101            2     Backup       100     100     None     101.1.1.100
[DeviceB] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan100            1     Backup       100     100     None     100.1.1.100
 Vlan101            2     Master       200     100     None     101.1.1.100
```

Verify that Device E has established OSPF neighbor relationships with Device A and Device B.

```
[DeviceE] display ospf peer

         OSPF Process 1 with Router ID 30.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 101.1.1.1       10.1.1.1        1   34         Full/DR           Vlan10
 101.1.1.2       20.1.1.1        1   36         Full/DR           Vlan20
```

Verify that a host in Area A can ping the host at 101.1.1.4 in Area B.

```
C:\Documents and Settings\Administrator>ping 101.1.1.4

Pinging 101.1.1.4 with 32 bytes of data:

Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126

Ping statistics for 101.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Verify that a host in Area A can ping VLAN-interface 30 (30.1.1.1) on Device E.

```
C:\Documents and Settings\Administrator>ping 30.1.1.1

Pinging 30.1.1.1 with 32 bytes of data:

Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 30.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Configuration files

IMPORTANT:
Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 101.1.1.0 0.0.0.255
#
vlan 10
#
vlan 100 to 101
#
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
 port drni group 1
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
 port drni group 2
#
interface Bridge-Aggregation125
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 100.1.1.100
 vrrp vrid 1 priority 200
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 150
#
```

```
interface Vlan-interface101
 ip address 101.1.1.1 255.255.255.0
 vrrp vrid 2 virtual-ip 101.1.1.100
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 port link-aggregation group 125
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 port link-aggregation group 125
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 10
#
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 123
 drni keepalive ip destination 1.1.1.2 source 1.1.1.1
#
 drni mad exclude interface GigabitEthernet1/0/5
#
 track 1 interface GigabitEthernet1/0/6
#
```

- Device B:

```
#
ospf 1
```

```
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 101.1.1.0 0.0.0.255
#
vlan 20
#
vlan 100 to 101
#
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
 port drni group 1
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
 port drni group 2
#
interface Bridge-Aggregation125
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 100.1.1.100
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 101.1.1.100
 vrrp vrid 2 priority 200
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 2 priority reduced 150
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 port link-aggregation group 125
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 to 101
 port link-aggregation group 125
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 20
#
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 123
 drni keepalive ip destination 1.1.1.1 source 1.1.1.2
#
 drni mad exclude interface GigabitEthernet1/0/5
#
 track 2 interface GigabitEthernet1/0/6
#
```

- Device C:

```
#
vlan 100
#
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
```

```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

- Device D:

```
#
vlan 101
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 101
#
```

- Device E:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
```

```
vlan 30
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface20
 ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface30
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
```

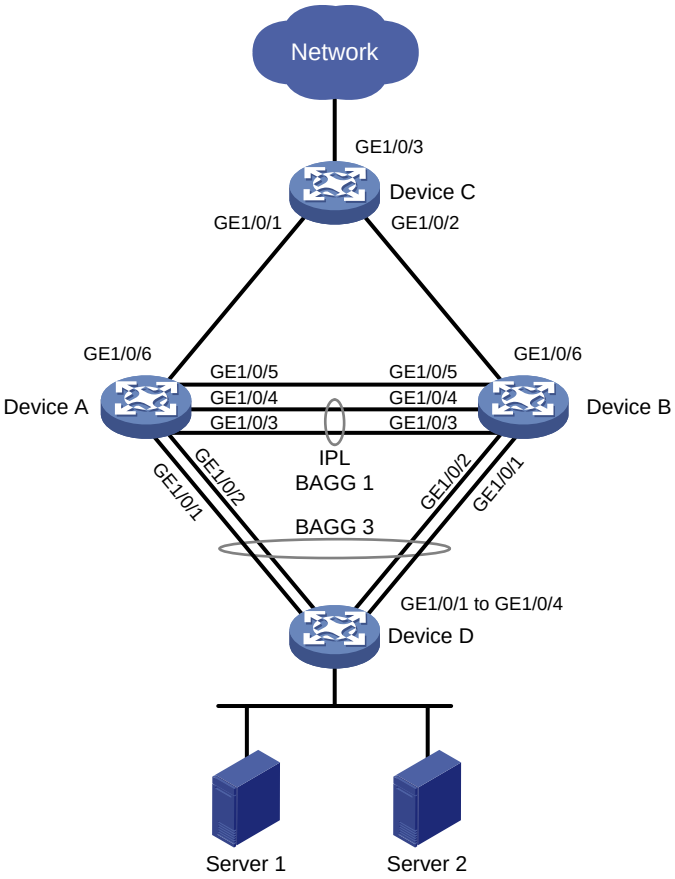
Example: Configuring IPv4 and IPv6 dual-active VLAN interfaces on a DR system

Network configuration

As shown in Figure 3, set up a DR system with Device A and Device B as follows.

- Attach Device D to DR interfaces on the DR system.
- Configure ECMP routes between the DR system and Device C.
- Configure dual-active VLAN interfaces on the DR system to provide IPv4 and IPv6 gateway services for the servers.

Figure 3 Network diagram



Device	Interface	IP address	Peer device and interface
Device A	GE1/0/1	-	Device D: GE1/0/1
	GE1/0/2	-	Device D: GE1/0/2
	GE1/0/3	-	Device B: GE1/0/3
	GE1/0/4	-	Device B: GE1/0/4
	GE1/0/5	IPv4: 21.1.1.1 IPv6: 21::1	Device B: GE1/0/5
	GE1/0/6	-	Device C: GE1/0/1
	Vlan-int100	IPv4: 100.1.1.100/24 IPv6: 100::100/64	-
	Vlan-int101	IPv4: 101.1.1.1/24 IPv6: 101::1/64	Device B: Vlan-int101 • IPv4: 101.1.1.2/24 • IPv6: 101::2/64
	Vlan-int32	IPv4: 32.1.1.1/24 IPv6: 32::1/64	Device C: Vlan-int32 • IPv4: 32.1.1.2/24 • IPv6: 32::2/64
Device B	GE1/0/1	-	Device D: GE1/0/3
	GE1/0/2	-	Device D: GE1/0/4

Device	Interface	IP address	Peer device and interface
	GE1/0/3	-	Device A: GE1/0/3
	GE1/0/4	-	Device A: GE1/0/4
	GE1/0/5	IPv4: 21.1.1.2 IPv6: 21::2	Device A: GE1/0/5
	GE1/0/6	-	Device C: GE1/0/6
	Vlan-int100	IPv4: 100.1.1.100/24 IPv6: 100::100/64	-
	Vlan-int101	IPv4: 101.1.1.2/24 IPv6: 101::2/64	Device A: Vlan-int101 • IPv4: 101.1.1.1/24 • IPv6: 101::1/64
	Vlan-int33	IPv4: 33.1.1.1/24 IPv6: 33::1/64	Device C: Vlan-int33 • IPv4: 33.1.1.2/24 • IPv6: 33::2/64
Device C	GE1/0/1	-	Device A: GE1/0/6
	GE1/0/2	-	Device B: GE1/0/6
	GE1/0/3	-	Network 1
	Vlan-int22	IPv4: 22.1.1.1/24 IPv6: 22::1/64	Network 1
	Vlan-int32	IPv4: 32.1.1.2/24 IPv6: 32::2/64	Device A: Vlan-int32 • IPv4: 32.1.1.1/24 • IPv6: 32::1/64
	Vlan-int33	IPv4: 33.1.1.2/24 IPv6: 33::2/64	Device B: Vlan-int33 • IPv4: 33.1.1.1/24 • IPv6: 33::1/64
Device D	GE1/0/1	-	Device A: GE1/0/1
	GE1/0/2	-	Device A: GE1/0/2
	GE1/0/3	-	Device B: GE1/0/1
	GE1/0/4	-	Device B: GE1/0/2

Analysis

To configure IPv4 and IPv6 dual-active VLAN interfaces, perform the following tasks:

- Assign the same IPv4 address, MAC address, IPv6 address, and IPv6 link-local address to VLAN-interface 100 interfaces on Device A and Device B.
- Create VLAN-interface 101 on both Device A and Device B for them to have Layer 3 connectivity. When an uplink to Device C fails, all traffic will be processed by the available DR member device.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

For two DR member devices to be identified as one DR system, you must configure the same DR system MAC address on them. Make sure DR systems use unique DR system MAC addresses.

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **`reserve-vlan-interface`** command to reserve local VLAN interface resources. For

more information about the reserve-vlan-interface command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 0002-0002-0002
[DeviceA] drni system-number 1
[DeviceA] drni system-priority 123
```

Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ip destination 21.1.1.2 source 21.1.1.1
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IPv4 address and an IPv6 address. The IP addresses will be used as the source IP addresses of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 21.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/5] ipv6 address 21::1 64
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface gigabitethernet 1/0/5
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Bridge-Aggregation 1 as the IPP.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation1] undo port trunk permit vlan 1
[DeviceA-Bridge-Aggregation1] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3, and assign it to DR group 1.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] port drni group 1
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/2] quit
```

Create VLAN 100 and VLAN 101.

```
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port link-type trunk
[DeviceA-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceA-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceA-Bridge-Aggregation3] quit
```

Create VLAN-interface 100, and assign it an IPv4 address and a MAC address for it to act as an IPv4 gateway.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ip address 100.1.1.100 255.255.255.0
[DeviceA-Vlan-interface100] mac-address 0000-0010-0010
```

Assign VLAN-interface 100 an IPv6 address and a link-local address for it to act as an IPv6 gateway.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ipv6 address 100::100 64
[DeviceA-Vlan-interface100] ipv6 address FE80::80 link-local
```

Exclude VLAN-interface 100 from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface vlan-interface100
```

Create VLAN-interface 101 and assign it an IPv4 address and an IPv6 address for the device to communicate with the DR peer at Layer 3.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ip address 101.1.1.1 255.255.255.0
[DeviceA-Vlan-interface101] ipv6 address 101::1 64
[DeviceA-Vlan-interface101] quit
```

Exclude VLAN-interface 101 from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface vlan-interface101
```

Configure the router ID as 3.3.3.3.

```
[DeviceA] router id 3.3.3.3
```

Configure OSPF on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPF packets. The OSPF configuration enables the DR member devices to have IPv4 connectivity.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] silent-interface vlan-interface 100
[DeviceA-ospf-1] import-route direct
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] quit
```

```
[DeviceA-ospf-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ospf 1 area 0.0.0.0
[DeviceA-Vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ospf 1 area 0.0.0.0
[DeviceA-Vlan-interface101] quit
```

Configure OSPFv3 on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPFv3 packets. The OSPFv3 configuration enables the DR member devices to have IPv6 connectivity.

```
[DeviceA] ospfv3 1
[DeviceA-ospfv3-1] silent-interface vlan-interface 100
[DeviceA-ospfv3-1] import-route direct
[DeviceA-ospfv3-1] area 0
[DeviceA-ospfv3-1-area-0.0.0.0] quit
[DeviceA-ospfv3-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ospfv3 1 area 0.0.0.0
[DeviceA-Vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ospfv3 1 area 0.0.0.0
[DeviceA-Vlan-interface101] quit
```

Create VLAN 32, and assign GigabitEthernet 1/0/6 to the VLAN. The interface is an uplink member interface of the DR interface.

```
[DeviceA] vlan 32
[DeviceA-vlan32] quit
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-type trunk
[DeviceA-GigabitEthernet1/0/6] port trunk permit vlan 32
[DeviceA-GigabitEthernet1/0/6] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/6] quit
```

Create VLAN-interface 32, and assign the interface an IPv4 address and an IPv6 address. Enable OSPF and OSPFv3 on the interface.

```
[DeviceA] interface vlan-interface 32
[DeviceA-Vlan-interface32] ip address 32.1.1.1 255.255.255.0
[DeviceA-Vlan-interface32] ipv6 address 32::1 64
[DeviceA-Vlan-interface32] ospf 1 area 0
[DeviceA-Vlan-interface32] ospfv3 1 area 0
[DeviceA-Vlan-interface32] quit
```

Configuring Device B

Configure DR system settings.

```
<DeviceB> system-view
[DeviceB] drni system-mac 0002-0002-0002
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 123
```

Configure DR keepalive packet parameters.

```
[DeviceB] drni keepalive ip destination 21.1.1.1 source 21.1.1.2
```

Configure GigabitEthernet 1/0/5 as a routed (Layer 3) interface and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 21.1.1.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/5] ipv6 address 21::2 64
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/5) from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface gigabitethernet 1/0/5
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/4] quit
```

Configure Bridge-Aggregation 1 as the IPP.

```
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation1] undo port trunk permit vlan 1
[DeviceB-Bridge-Aggregation1] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3, and assign it to DR group 1.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] port drni group 1
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/2] quit
```

Create VLAN 100 and VLAN 101.

```
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] vlan 101
[DeviceB-vlan101] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port link-type trunk
```

```
[DeviceB-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceB-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceB-Bridge-Aggregation3] quit
```

Create VLAN-interface 100, and assign it an IPv4 address and a MAC address for it to act as an IPv4 gateway.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ip address 100.1.1.100 255.255.255.0
[DeviceB-Vlan-interface100] mac-address 0000-0010-0010
```

Assign VLAN-interface 100 an IPv6 address and a link-local address for it to act as an IPv6 gateway.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ipv6 address 100::100 64
[DeviceB-Vlan-interface100] ipv6 address FE80::80 link-local
```

Exclude VLAN-interface 100 from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface vlan-interface100
```

Create VLAN-interface 101 and assign it an IPv4 address and an IPv6 address for the device to communicate with the DR peer at Layer 3.

```
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ip address 101.1.1.2 24
[DeviceB-vlan-interface101] ipv6 address 101::2 64
[DeviceB-vlan-interface101] quit
```

Exclude VLAN-interface 101 from the shutdown action by DRNI MAD.

```
[DeviceB] drni mad exclude interface vlan-interface101
```

Configure the router ID as 4.4.4.4.

```
[DeviceB] router id 4.4.4.4
```

Configure OSPF on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPF packets. The OSPF configuration enables the DR member devices to have IPv4 connectivity.

```
[DeviceB] ospf 1
[DeviceB-ospf-1] silent-interface vlan-interface100
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ospf 1 area 0.0.0.0
[DeviceB-Vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] ospf 1 area 0.0.0.0
[DeviceB-Vlan-interface101] quit
```

Configure OSPFv3 on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPFv3 packets. The OSPFv3 configuration enables the DR member devices to have IPv6 connectivity.

```
[DeviceB] ospfv3 1
[DeviceB-ospf-1] silent-interface vlan-interface100
[DeviceB-ospfv3-1] import-route direct
[DeviceB-ospfv3-1] area 0
[DeviceB-ospfv3-1-area-0.0.0.0] quit
```

```
[DeviceB-ospfv3-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-vlan-interface100] ospfv3 1 area 0
[DeviceB-vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ospfv3 1 area 0
[DeviceB-vlan-interface101] quit
```

Create VLAN 33, and assign GigabitEthernet 1/0/6 to the VLAN. The interface is an uplink member interface of the DR interface.

```
[DeviceB] vlan 33
[DeviceB-vlan33] quit
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port link-type trunk
[DeviceB-GigabitEthernet1/0/6] port trunk permit vlan 33
[DeviceB-GigabitEthernet1/0/6] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/6] quit
```

Create VLAN-interface 33, and assign the interface an IPv4 address and an IPv6 address. Enable OSPF and OSPFv3 on the interface.

```
[DeviceB] interface vlan-interface 33
[DeviceB-Vlan-interface33] ip address 33.1.1.1 255.255.255.0
[DeviceB-Vlan-interface33] ipv6 address 33::1 64
[DeviceB-Vlan-interface33] ospf 1 area 0
[DeviceB-Vlan-interface33] ospfv3 1 area 0
[DeviceB-Vlan-interface33] quit
```

Configuring Device C

Create VLAN 32 and assign GigabitEthernet 1/0/1 (attached to Device A) to the VLAN. Create VLAN-interface 32 and assign it an IPv4 address and an IPv6 address.

```
<DeviceC> system-view
[DeviceC] vlan 32
[DeviceC-vlan32] quit
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 32
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ip address 32.1.1.2 24
[DeviceC-Vlan-interface32] ipv6 address 32::2 64
[DeviceC-Vlan-interface32] quit
```

Create VLAN 33 and assign GigabitEthernet 1/0/2 (attached to Device B) to the VLAN. Create VLAN-interface 33 and assign it an IPv4 address and an IPv6 address.

```
[DeviceC] vlan 33
[DeviceC-vlan33] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 33
```

```
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface33] ip address 33.1.1.2 24
[DeviceC-Vlan-interface33] ipv6 address 33::2 64
[DeviceC-Vlan-interface33] quit
```

Configure the router ID as 5.5.5.5.

```
[DeviceC] router id 5.5.5.5
```

Enable OSPF on VLAN-interface 32 and VLAN-interface 33.

```
[DeviceC] ospf 1
[DeviceC-ospf-1] import-route direct
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ospf 1 area 0
[DeviceC-Vlan-interface32] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface33] ospf 1 area 0
[DeviceC-Vlan-interface33] quit
```

Enable OSPFv3 on VLAN-interface 32 and VLAN-interface 33.

```
[DeviceC] ospfv3 1
[DeviceC-ospfv3-1] import-route direct
[DeviceC-ospfv3-1] area 0
[DeviceC-ospfv3-1-area-0.0.0.0] quit
[DeviceC-ospfv3-1] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ospfv3 1 area 0
[DeviceC-Vlan-interface32] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface33] ospfv3 1 area 0
[DeviceC-Vlan-interface33] quit
```

Create VLAN 22, and assign GigabitEthernet 1/0/3 (attached to the upstream network) to the VLAN. Create VLAN-interface 22 and assign it an IPv4 address and an IPv6 address.

```
[DeviceC] vlan 22
[DeviceC-vlan22] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 22
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface vlan-interface 22
[DeviceC-Vlan-interface22] ip address 22.1.1.1 24
[DeviceC-Vlan-interface22] ipv6 address 22::1 64
[DeviceC-Vlan-interface22] quit
```

Configuring Device D

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
<DeviceD> system-view
[DeviceD] interface bridge-aggregation 3
[DeviceD-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to aggregation group 3.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceD-if-range] port link-aggregation group 3
[DeviceD-if-range] quit
```

Create VLAN 100.

```
[DeviceD] vlan 100
[DeviceD-vlan100] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceD] interface bridge-aggregation 3
[DeviceD-Bridge-Aggregation3] port link-type trunk
[DeviceD-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceD-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceD-Bridge-Aggregation3] quit
```

Verifying the configuration

Verifying the DRNI configuration

The following tasks use Device A as an example.

Verify that Device A has formed a DR system with Device B.

```
[DeviceA] display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG1
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time (s)
BAGG3         1         UP                   UP          -
```

Verify that the keepalive link is operating correctly.

```
[DeviceA] display drni keepalive
Neighbor keepalive link status: Up
Neighbor is alive for: 64765 s 28 ms
Keepalive packet transmission status:
  Sent: Successful
  Received: Successful
Last received keepalive packet information:
  Source IP address: 21.1.1.2
```

```
  Time: 2021/01/17 17:10:52
  Action: Accept

Distributed relay keepalive parameters:
Destination IP address: 21.1.1.2
Source IP address: 21.1.1.1
Keepalive UDP port : 6400
Keepalive VPN name : N/A
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Verify that the DR system is operating correctly.

```
<Sysname> display drni system
                     System information
Local system number: 1                      Peer system number: 2
Local system MAC: 0002-0002-0002            Peer system MAC: 0002-0002-0002
Local system priority: 123                  Peer system priority: 123
Local bridge MAC: 3cd4-3ce1-0200            Peer bridge MAC: 3cd4-437d-0300
Local effective role: Primary               Peer effective role: Secondary
Health level: 0
Standalone mode on split: Disabled
In standalone mode: No

                     System timer information
Timer                       State       Value (s)    Remaining time (s)
Auto recovery               Disabled    -            -
Restore delay               Disabled    30           -
Consistency-check delay     Disabled    15           -
Standalone delay            Disabled    -            -
Role to None delay          Disabled    60           -
```

Verify that the interfaces used by DRNI are operating correctly.

```
[DeviceA] display drni verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired

IPP/IPP ID: BAGG1/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (27), GE1/0/4 (32)
Peer Selected ports indexes: 125, 130

DR interface/DR group ID: BAGG3/1
Local DR interface state: UP
Peer DR interface state: UP
DR group state: UP
Local DR interface down cause: -
```

```
Remaining DRNI DOWN time: -
Local DR interface LACP MAC: Config=N/A, Effective=0002-0002-0002
Peer DR interface LACP MAC: Config=N/A, Effective=0002-0002-0002
Local DR interface LACP priority: Config=32768, Effective=123
Peer DR interface LACP priority: Config=32768, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (12), GE1/0/2 (13)
Peer Selected ports indexes: 56, 57
```

Verifying routing configuration

Verify that Device A have established OSPF neighbor relationships.

```
[DeviceA] display ospf peer

         OSPF Process 1 with Router ID 3.3.3.3
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 4.4.4.4         101.1.1.2       1   36         Full/DR           Vlan101
 5.5.5.5         32.1.1.2        1   38         Full/DR           Vlan32
```

Verify that Device A have established OSPFv3 neighbor relationships.

```
[DeviceA] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 4.4.4.4         1   Full/DR           00:00:36  0      Vlan101
 5.5.5.5         1   Full/DR           00:00:35  0      Vlan32
```

Verify that Device B have established OSPF neighbor relationships.

```
[DeviceB] display ospf peer

         OSPF Process 1 with Router ID 4.4.4.4
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         101.1.1.1       1   32         Full/BDR          Vlan101
 5.5.5.5         33.1.1.2        1   33         Full/DR           Vlan33
```

Verify that Device B have established OSPFv3 neighbor relationships.

```
[DeviceB] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
```

```
---------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 3.3.3.3         1   Full/BDR         00:00:35  0      Vlan101
 5.5.5.5         1   Full/DR          00:00:38  0      Vlan33
```

Verify that Device C have established OSPF neighbor relationships.

```
[DeviceC] display ospf peer

         OSPF Process 1 with Router ID 5.5.5.5
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         32.1.1.1        1   32         Full/DR           Vlan32
 4.4.4.4         33.1.1.1        1   38         Full/DR           Vlan33
```

Verify that Device C have established OSPFv3 neighbor relationships.

```
[DeviceC] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 5.5.5.5

 Area: 0.0.0.0
---------------------------------------------------------------------------
 Router ID       Pri State            Dead-Time InstID Interface
 3.3.3.3         1   Full/DR          00:00:37  0      Vlan32
 4.4.4.4         1   Full/DR          00:00:34  0      Vlan33
```

Verifying network connectivity

Verify that Server 1 and Server 2 have both IPv4 and IPv6 connectivity to the upstream network connected to Device C.

Verifying traffic failover

Disconnect the uplink interface on Device A and verify that Server 1 and Server 2 have connectivity to the upstream network connected to Device C. Transient traffic loss will occur during traffic failover.

Configuration files

- Device A:

```
#
 router id 3.3.3.3
#
ospf 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
ospfv3 1
 import-route direct
```

```
 silent-interface Vlan-interface100
 area 0.0.0.0
#
vlan 1
#
vlan 32
#
vlan 100 to 101
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
 port drni group 1
#
interface Vlan-interface32
 ip address 32.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 32::1/64
#
interface Vlan-interface100
 ip address 100.1.1.100 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 mac-address 0000-0010-0010
 ipv6 address FE80::80 link-local
 ipv6 address 100::100/64
#
interface Vlan-interface101
 ip address 101.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 101::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```

```
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port link-aggregation group 1
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 21.1.1.1 255.255.255.0
 ipv6 address 21::1/64
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 32
#
 drni system-mac 0002-0002-0002
 drni system-number 1
 drni system-priority 123
 drni keepalive ip destination 21.1.1.2 source 21.1.1.1
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface100
 drni mad exclude interface Vlan-interface101
#
```

- Device B:

```
#
 router id 4.4.4.4
#
```

```
ospf 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
ospfv3 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
vlan 1
#
vlan 33
#
vlan 100 to 101
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
 port drni group 1
#
interface Vlan-interface33
 ip address 33.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 33::1/64
#
interface Vlan-interface100
 ip address 100.1.1.100 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 mac-address 0000-0010-0010
 ipv6 address FE80::80 link-local
 ipv6 address 100::100/64
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 101::2/64
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 21.1.1.2 255.255.255.0
 ipv6 address 21::2/64
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 33
#
 drni system-mac 0002-0002-0002
 drni system-number 2
 drni system-priority 123
 drni keepalive ip destination 21.1.1.1 source 21.1.1.2
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface100
 drni mad exclude interface Vlan-interface101
#
```

- Device C:

```
#
 router id 5.5.5.5
#
ospf 1
 import-route direct
 area 0.0.0.0
#
ospfv3 1
 import-route direct
 area 0.0.0.0
#
vlan 1
#
vlan 22
#
vlan 32 to 33
#
interface Vlan-interface22
 ip address 22.1.1.1 255.255.255.0
 ipv6 address 22::1/64
#
interface Vlan-interface32
 ip address 32.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 32::2/64
#
interface Vlan-interface33
 ip address 33.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 33::2/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 32
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 33
#
interface GigabitEthernet1/0/3
 port link-mode bridge
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 22
#
```

- Device D:

```
#
vlan 1
#
vlan 100
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
```

Contents

Introduction

This document provides examples for setting up an IRF 3.1 system.

IRF 3.1 integrates multiple lower-layer devices with a higher-layer IRF fabric to provide high-density, low-cost connectivity at the access layer. IRF 3.1 is implemented based on IEEE 802.1BR.

In an IRF 3.1 system, the higher-layer IRF fabric is called the parent fabric and the lower-layer devices are called bridge port extenders (PEXs). You manage and configure the PEXs from the parent fabric as if they were interface modules on the parent fabric.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IRF 3.1.

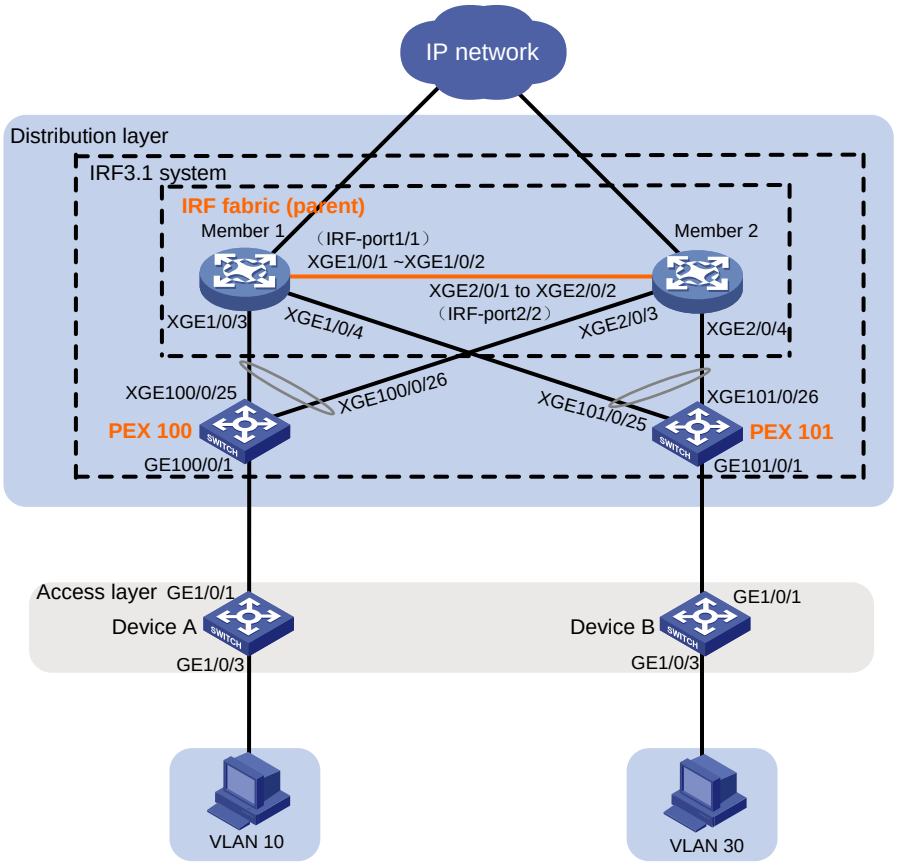
Example: Setting up an IRF 3.1 system

Network configuration

As shown in Figure 1:

- Use Member 1 and Member 2 to set up an IRF fabric at the distribution layer.
- Use the IRF fabric as the parent fabric and attach PEXs to the parent fabric to set up an IRF 3.1 system.
- The IRF 3.1 system acts as the gateway for users in VLANs 10 and 30.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported

Hardware	Software version
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Supported: Release 63xx, Release 65xx Not supported: Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series	Not supported

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series IE4520 switch series	Not supported
S5135S-EI switch	Not supported

Parent IRF fabric and PEX hardware compatibility

Parent IRF fabric	PEX
S5560X-EI switch series	• S5560X-EI switch series • FS4100 Switch Series
S5560X-HI switch series	FS4100 switch series
S6520X-HI switch series S6520X-EI switch series	FS4100 switch series
S6520X-SI switch series S6520-SI switch series	FS4100 switch series
S5000-EI switch series	FS4100 switch series
MS4600 switch series	FS4100 switch series
ES5500 switch series	ES4100 switch series

Restrictions and guidelines

To assign extended ports on multiple PEXs to the same Layer 2 extended-link aggregation group, make sure the PEXs meet the following requirements:

- The PEXs belong to the same switch series.
- The PEXs are in the same PEX group.
- The PEXs are at the same tier.

The FS4100 switch series and ES4100 switch series do not support Layer 2 extended-link aggregate interfaces. You can connect a downstream access device to an FS4100 or ES4100 PEX only through a single link.

Prerequisites

On PEXs, only some high-speed ports can act as member interfaces of upstream ports. Before you set up an IRF 3.1 system, use either of the following methods to identify these ports and select upstream member interfaces from among them as needed:

- If you have not placed the switch in PEX mode, use the virtual technologies configuration guide (or IRF configuration guide) for the switch to identify candidate upstream member interfaces.
- If the switch has been placed in PEX mode, identify the candidate upstream member interfaces from the CLI:
  a. Execute the **probe** command to enter probe view.
  b. Execute the **display system internal pex upstreamport** command.

Table 1 lists the candidate upstream member interfaces on the PEXs to which this example is applicable:

Table 1 Candidate upstream member interfaces on the PEXs

PEX	Candidate upstream member interfaces
S5560X-EI switch series	The two highest numbered ports on the front panel
FS4100 switch series	The two highest numbered ports on the front panel
ES4100 switch series	The two highest numbered 10/100/1000BASE-T autosensing Ethernet ports and the two highest numbered SFP ports. Make sure the upstream member interfaces belong to the same type.

Procedures

Setting up the parent fabric

1. Configure Member 1:

   # Place the device in 802.1BR mode.

   ```
   <Sysname> system-view
   [Sysname] switch-mode 2
   ```

   # Set the device operating mode to switch mode. This step is required only for setting up an S5560X-EI parent IRF fabric.

   ```
   [Sysname] pex system-working-mode switch
   ```

Shut down Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.

```
[Sysname] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to IRF-port 1/1.

```
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/2
[Sysname-irf-port1/1] quit
```

Bring up Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 1/0/1 to ten-gigabitethernet 1/0/2
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Activate the IRF port configuration.

```
[Sysname] irf-port-configuration active
```

2. Configure Member 2:

Place the device in 802.1BR mode.

```
<Sysname> system-view
[Sysname] switch-mode 2
```

Set the device operating mode to switch mode. This step is required only for setting up an S5560X-EI parent IRF fabric.

```
[Sysname] pex system-working-mode switch
```

Change the IRF member ID to 2 and reboot the device for the new member ID to take effect.

```
[Sysname] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y
[Sysname] quit
<Sysname> reboot
```

Log in to the device and shut down Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/2.

```
<Sysname> system-view
[Sysname] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/2
[Sysname-if-range] shutdown
[Sysname-if-range] quit
```

Bind Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/2 to IRF-port 2/2.

```
[Sysname] irf-port 2/2
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/1
[Sysname-irf-port2/2] port group interface ten-gigabitethernet 2/0/2
[Sysname-irf-port2/2] quit
```

Bring up Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/2 and save the configuration.

```
[Sysname] interface range ten-gigabitethernet 2/0/1 to ten-gigabitethernet 2/0/2
[Sysname-if-range] undo shutdown
[Sysname-if-range] quit
[Sysname] save
```

Connect the IRF physical interfaces on Member 2 to the IRF physical interfaces on Member 1. (Details not shown.)

Activate the IRF port configuration on Member 2.

```
[Sysname] irf-port-configuration active
```

Member 1 and Member 2 perform master election. The device that fails the election will reboot automatically to form an IRF fabric with the other device.

Configuring cascade ports for PEXs on the parent fabric

Enter system view.

```
<Sysname> system-view
```

Enable LLDP globally.

```
[Sysname] lldp global enable
```

Create PEX group 1.

```
[Sysname] pex group 1
[Sysname-pex-group-1] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 100. The aggregate interface will act as the cascade port connecting to the PEX in slot 100. For easy maintenance, this example assigns the aggregate interface the same number as the PEX virtual slot.

```
[Sysname] interface bridge-aggregation 100
```

Enable PEX connection capability on Bridge-Aggregation 100 and assign Bridge-Aggregation 100 to PEX group 1.

```
[Sysname-Bridge-Aggregation100] pex-capability enable group 1
The aggregate interface was automatically set to dynamic aggregation mode and configured as an STP edge port.
```

Assign virtual slot number 100 to the PEX.

```
[Sysname-Bridge-Aggregation100] pex associate slot 100
[Sysname-Bridge-Aggregation100] quit
```

Enable LLDP on Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 2/0/3 in interface range view. By default, LLDP is enabled on a port.

```
[Sysname] interface range ten-gigabitethernet 1/0/3 ten-gigabitethernet 2/0/3
[Sysname-if-range] lldp enable
```

Assign Ten-GigabitEthernet 1/0/3 and Ten-GigabitEthernet 2/0/3 to aggregation group 100. The ports will act as the cascade member interfaces.

```
[Sysname-if-range] port link-aggregation group 100
[Sysname-if-range] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 101. The aggregate interface will act as the cascade port connecting to the PEX in slot 101.

```
[Sysname] interface bridge-aggregation 101
```

Enable PEX connection capability on Bridge-Aggregation 101 and assign the interface to PEX group 1.

```
[Sysname-Bridge-Aggregation101] pex-capability enable group 1
The aggregate interface was automatically set to dynamic aggregation mode and configured as an STP edge port.
```

Assign virtual slot number 101 to the PEX.

```
[Sysname-Bridge-Aggregation101] pex associate slot 101
[Sysname-Bridge-Aggregation101] quit
```

Enable LLDP on Ten-GigabitEthernet 1/0/4 and Ten-GigabitEthernet 2/0/4 in interface range view. By default, LLDP is enabled on a port.

```
[Sysname] interface range ten-gigabitethernet 1/0/4 ten-gigabitethernet 2/0/4
```

```
[Sysname-if-range] lldp enable
```

Assign Ten-GigabitEthernet 1/0/4 and Ten-GigabitEthernet 2/0/4 to aggregation group 101. The ports will act as the cascade member interfaces.

```
[Sysname-if-range] port link-aggregation group 101
[Sysname-if-range] quit
```

Configuring PEXs

Configure the devices to be used as PEXs to operate in auto or PEX mode. This example uses PEX 100 to describe the configuration procedure. You configure PEX 101 in the same way PEX 100 is configured.

1. Configure PEX 100 to operate in auto mode:

IMPORTANT:

Skip this step if the PEXs are FS4100 switches or ES4100 switches.

Change the operating mode to auto mode. By default, the operating mode is auto.

```
<Sysname> system-view
[Sysname] pex system-working-mode auto
```

Save the running configuration.

```
[Sysname] save
```

2. Select upstream member interfaces.

   In this example, Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26 are used. For information about candidate upstream member interfaces, see the configuration and installation guides for the PEX. (Details not shown.)

3. Connect the upstream member interfaces on PEX 100 to the cascade member interfaces on the parent fabric as shown in Figure 1. (Details not shown.)

Configuring the gateway settings on the IRF 3.1 system

Enter system view.

```
<Sysname> system-view
```

Create VLANs 10 and 30.

```
[Sysname] vlan 10 30
```

Create VLAN-interface 10 and assign IP address 192.168.1.1/24 to the VLAN interface.

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 192.168.1.1 24
[Sysname-Vlan-interface10] quit
```

Create VLAN-interface 30 and assign IP address 192.168.3.1/24 to the VLAN interface.

```
[Sysname] interface vlan-interface 30
[Sysname-Vlan-interface30] ip address 192.168.3.1 24
[Sysname-Vlan-interface30] quit
```

Assign GigabitEthernet 100/0/1 to VLAN 10.

```
[Sysname] interface gigabitethernet 100/0/1
[Sysname-GigabitEthernet100/0/1] port access vlan 10
[Sysname-GigabitEthernet100/0/1] quit
```

Assign GigabitEthernet 101/0/1 to VLAN 30.

```
[Sysname] interface gigabitethernet 101/0/1
```

```
[Sysname-GigabitEthernet101/0/1] port access vlan 30
[Sysname-GigabitEthernet101/0/1] quit
```

Configuring access layer devices

1. Configure Device A:

   # Enter system view.

   ```
   <Sysname> system-view
   ```

   # Create VLAN 10.

   ```
   [Sysname] vlan 10
   [Sysname-vlan10] quit
   ```

   # Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to VLAN 10.

   ```
   [Sysname] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/3
   [Sysname-if-range] port access vlan 10
   [Sysname-if-range] quit
   ```

2. Configure Device B:

   # Enter system view.

   ```
   <Sysname> system-view
   ```

   # Create VLAN 30.

   ```
   [Sysname] vlan 30
   [Sysname-vlan30] quit
   ```

   # Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3 to VLAN 30.

   ```
   [Sysname] interface range gigabitethernet 1/0/1 gigabitethernet 1/0/3
   [Sysname-if-range] port access vlan 30
   [Sysname-if-range] quit
   ```

Verifying the configuration

Use the **`display device`** command to display device information on the parent fabric. If the IRF 3.1 system has been set up, the system displays information about both parent IRF member devices and PEXs. (Details not shown.)

Test the gateway service of the IRF 3.1 system. Verify that hosts in VLANs 10 and 30 can ping each other. (Details not shown.)

Configuration files

- IRF 3.1 system:

  ```
  #
   pex group 1
  #
   lldp global enable
  #
   pex system-working-mode switch
  #
  vlan 10
  #
  vlan 30
  ```

```
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/1
 port group interface Ten-GigabitEthernet1/0/2
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/1
 port group interface Ten-GigabitEthernet2/0/2
#
interface Bridge-Aggregation100
 pex-capability enable group 1
 pex associate slot 100
 link-aggregation mode dynamic
 stp edged-port
#
interface Bridge-Aggregation101
 pex-capability enable group 1
 pex associate slot 101
 link-aggregation mode dynamic
 stp edged-port
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet100/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet101/0/1
 port link-mode bridge
 port access vlan 30
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port link-aggregation group 100
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port link-aggregation group 101
#
interface Ten-GigabitEthernet2/0/3
 port link-mode bridge
 port link-aggregation group 100
#
interface Ten-GigabitEthernet2/0/4
```

```
 port link-mode bridge
 port link-aggregation group 101
```

- Device A:

```
#
vlan 10
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
```

- Device B:

```
#
vlan 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
```

Contents

Introduction

This document provides PTP configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of PTP.

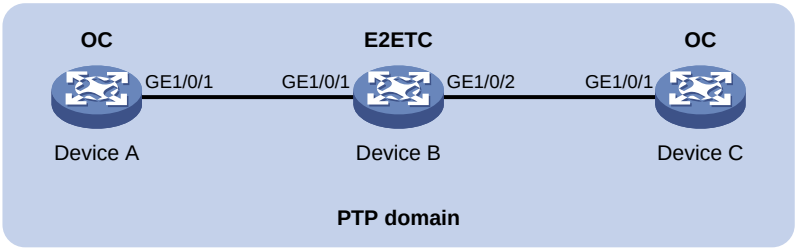
Example: Configuring Layer 2 IEEE 1588v2 PTP

Network configuration

As shown in Figure 1, a PTP domain contains Device A, Device B, and Device C. Configure Layer 2 IEEE 1588v2 PTP as follows for time synchronization:

- Specify the IEEE 1588v2 PTP profile for the devices.
- Specify the OC clock node type for Device A and Device C, and E2ETC clock node type for Device B. These clock nodes elect a GM through BMC based on their respective default GM attributes.
- Use the default Request-Response delay measurement mechanism for Device A and Device C.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx

Hardware	Software version
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported

Hardware	Software version
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	Not supported
IE4300-28P-M switch IE4320-28P switch	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Not supported

Procedures

Configuring Device A

Specify the IEEE 1588v2 PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile 1588v2
```

Specify the OC clock node type.

```
[DeviceA] ptp mode oc
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Specify a PTP domain.

```
[DeviceA] ptp domain 0
```

Specify PTP for obtaining the time.

```
[DeviceA] clock protocol ptp
```

Enable PTP on GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ptp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Specify the IEEE 1588v2 PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile 1588v2
```

Specify the E2ETC clock node type.

```
[DeviceB] ptp mode e2etc
```

Specify a PTP domain.

```
[DeviceB] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceB] clock protocol ptp
```

Enable PTP on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ptp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Enable PTP on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ptp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Specify the IEEE 1588v2 PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile 1588v2
```

Specify the OC clock node type.

```
[DeviceC] ptp mode oc
```

Specify a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceC] clock protocol ptp
```

Enable PTP on GigabitEthernet 1/0/1.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ptp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.

When the network topology is stable, perform the following tasks to verify the PTP configuration:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief information about PTP interfaces.

  # Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : OC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

  # Display brief information about PTP interfaces on Device A.

```
[DeviceA] display ptp interface brief
Name      InstID    State        Delay mechanism  Clock step  Asymmetry correction
GE1/0/1    0         Master        E2E              Two         0
```

  # Display PTP clock information on Device B.

```
[DeviceB] display ptp clock
PTP global state    : Enabled
```

```
PTP profile         : IEEE 1588 Version 2
PTP mode            : E2ETC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
Offset from master : N/A
Mean path delay    : N/A
Steps removed      : N/A
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device B.

```
[DeviceB] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         N/A           E2E              Two         0
GE1/0/2  0         N/A           E2E              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : OC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0002
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
Offset from master : 25
Mean path delay    : 323
Steps removed      : 2
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device C.

```
[DeviceC] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Slave         E2E              Two         0
```

The command outputs show that Device A is elected as the GM and GigabitEthernet1/0/1 on Device A is the master port.

Configuration files

- Device A and Device C:

```
#
 clock protocol ptp
#
 ptp profile 1588v2
 ptp mode oc
#
interface GigabitEthernet 1/0/1
 ptp enable
#
```

- Device B:

```
#
 clock protocol ptp
#
 ptp profile 1588v2
 ptp mode e2etc
#
interface GigabitEthernet 1/0/1
 ptp enable
#
interface GigabitEthernet 1/0/2
 ptp enable
#
```

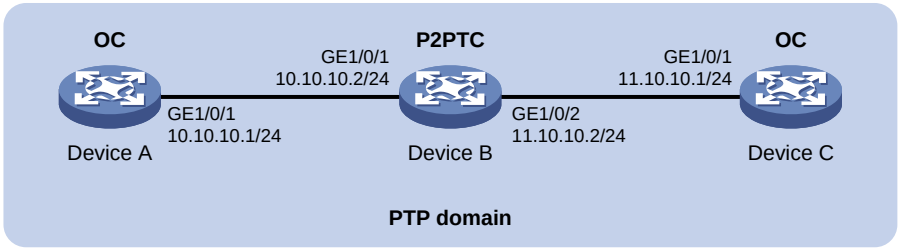
Example: Configuring Layer 3 IEEE 1588v2 PTP in multicast mode

Network configuration

As shown in Figure 2, a PTP domain contains Device A, Device B, and Device C. Configure Layer 3 IEEE 1588v2 PTP in multicast mode as follows for time synchronization:

- Specify the IEEE 1588v2 PTP profile for the devices.
- Specify the OC clock node type for Device A and Device C, and the P2PTC clock node type for Device B. These clock nodes elect a GM through BMC based on their respective default GM attributes.
- Configure the multicast PTP transport mode and UDP (IPv4) transport protocol for the devices.
- Configure the peer delay measurement mechanism (p2p) for Device A and Device C.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Release 6615Pxx, and Release 6628Pxx
S5570S-EI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported

Hardware	Software version
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch	Not supported

Hardware	Software version
IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	
IE4300-28P-M switch IE4320-28P switch	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Not supported

Procedures

Configuring Device A

Specify the IEEE 1588v2 PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile 1588v2
```

Specify the OC clock node type.

```
[DeviceA] ptp mode oc
```

Specify a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceA] ptp source 10.10.10.1
```

Specify PTP for obtaining the time.

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify the UDP (IPv4) transport protocol and the peer delay measurement mechanism (p2p) and enable PTP.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ptp transport-protocol udp [DeviceA-GigabitEthernet1/0/1] ptp delay-mechanism p2p
[DeviceA-GigabitEthernet1/0/1] ptp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Specify the IEEE 1588v2 PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile 1588v2
```

Specify the P2PTC clock node type.

```
[DeviceB] ptp mode p2ptc
```

Specify a PTP domain.

```
[DeviceB] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceB] ptp source 10.10.10.2
```

Specify PTP for obtaining the time.

```
[DeviceB] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify the UDP (IPv4) transport protocol and enable PTP.

```
[DeviceB] interface gigabitethernet 1/0/1
DeviceB-GigabitEthernet1/0/1] ptp transport-protocol udp
[DeviceB-GigabitEthernet1/0/1] ptp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

On GigabitEthernet 1/0/2, specify the UDP transport protocol and enable PTP.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ptp transport-protocol udp
[DeviceB-GigabitEthernet1/0/2] ptp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Specify the IEEE 1588v2 PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile 1588v2
```

Specify the OC clock node type.

```
[DeviceC] ptp mode oc
```

Specify a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceC] ptp source 11.10.10.1
```

Specify PTP for obtaining the time.

```
[DeviceC] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify the UDP (IPv4) transport protocol and the peer delay measurement mechanism (p2p) and enable PTP.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ptp transport-protocol udp [DeviceC-GigabitEthernet1/0/1] ptp delay-mechanism p2p
[DeviceC-GigabitEthernet1/0/1] ptp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.

When the network topology is stable, perform the following tasks to verify the PTP configuration:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief information about PTP interfaces.

  # Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : OC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

  # Display brief information about PTP interfaces on Device A.

```
[DeviceA] display ptp interface brief
Name      InstID    State        Delay mechanism  Clock step  Asymmetry correction
GE1/0/1    0         Master        P2P              Two         0
```

  # Display PTP clock information on Device B.

```
[DeviceB] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : P2PTC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
Offset from master : N/A
```

```
Mean path delay    : N/A
Steps removed      : N/A
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device B.

```
[DeviceB] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         N/A           P2P              Two         0
GE1/0/2  0         N/A           P2P              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : OC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0002
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device C.

```
[DeviceC] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Slave         P2P              Two         0
```

The command outputs show that Device A is elected as the GM and GigabitEthernet1/0/1 on Device A is the master port.

Configuration files

- Device A:

```
#
 clock protocol ptp
#
 ptp profile 1588v2
 ptp mode oc
 ptp source 10.10.10.1
#
interface GigabitEthernet 1/0/1
 ptp delay-mechanism p2p
```

```
 ptp transport-protocol udp
 ptp enable
#
```

- Device B:

```
#
 clock protocol ptp
#
 ptp profile 1588v2
 ptp mode p2ptc
 ptp source 10.10.10.2
#
interface GigabitEthernet 1/0/1
 ptp transport-protocol udp
 ptp enable
#
interface GigabitEthernet 1/0/2
 ptp transport-protocol udp
 ptp enable
#
```

- Device C:

```
#
 clock protocol ptp
#
 ptp profile 1588v2
 ptp mode oc
 ptp source 11.10.10.1
#
interface GigabitEthernet 1/0/1
 ptp delay-mechanism p2p
 ptp transport-protocol udp
 ptp enable
#
```

Example: Configuring Layer 3 IEEE 1588v2 PTP in unicast mode

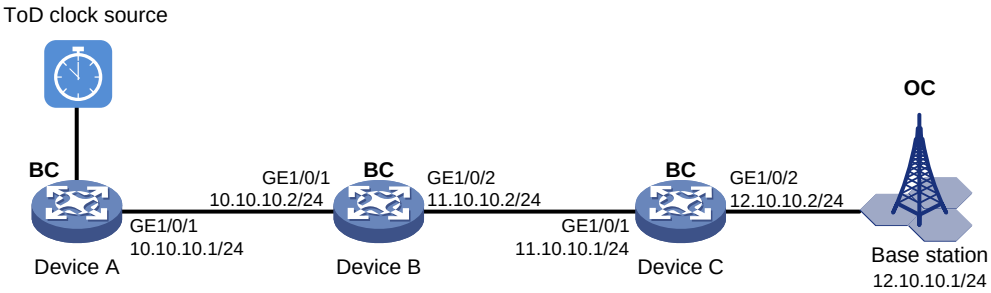
Network configuration

As shown in Figure 3, configure PTP (IEEE 1588 version 2, IPv4 UDP transport, unicast transmission) to enable Device A, Device B, Device C, and the base station to synchronize the time with the ToD clock source.

- Specify the IEEE 1588 version 2 PTP profile and unicast IPv4 UDP transport of PTP messages for Device A, Device B, and Device C.
- Assign Device A, Device B, Device C, and the base station to PTP domain 0. Specify the BC clock node type for Device A, Device B, and Device C.
- Connect Device A to the ToD clock source and Device C to the base station.

- Use the default Request_Response delay measurement mechanism on all clock nodes in the PTP domain.

Figure 3 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Not supported
MS4520V2-30F	Not supported
MS4520V2-30C MS4520V2-54C	Not supported
MS4520V2-28S MS4520V2-24TP	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported

S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported

IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	Not supported
IE4300-28P-M IE4320-28P	Not supported
IE4520 series	Not supported
S5135S-EI series	Not supported

Procedures

IMPORTANT:

The device does not provide ToD interfaces. It can be deployed as Device B or Device C but not Device A.

Before configuration, assign IP addresses to the interfaces, and make sure the devices can reach each other. (Details not shown.)

Configuring Device A

Specify the IEEE 1588 version 2 PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile 1588v2
```

Specify the BC clock node type.

```
[DeviceA] ptp mode bc
```

Create a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Configure the device to use ToD 0 to receive clock signals and set the receive delay correction to 1000 nanoseconds.

```
[DeviceA] ptp tod0 input delay 1000
```

Set priority 1 to **0** for the ToD 0 clock.

```
[DeviceA] ptp priority clock-source tod0 priority1 0
```

On GigabitEthernet 1/0/1, specify IPv4 UDP transport of PTP messages, configure the destination IP address for unicast PTP messages, and enable PTP.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ptp transport-protocol udp
[DeviceA-GigabitEthernet1/0/1] ptp unicast-destination 10.10.10.2
[DeviceA-GigabitEthernet1/0/1] ptp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Specify the IEEE 1588 version 2 PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile 1588v2
```

Specify the BC clock node type.

```
[DeviceB] ptp mode bc
```

Create a PTP domain.

```
[DeviceB] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify IPv4 UDP transport of PTP messages, configure the destination IP address for unicast PTP messages, and enable PTP.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ptp transport-protocol udp
[DeviceB-GigabitEthernet1/0/1] ptp unicast-destination 10.10.10.1
[DeviceB-GigabitEthernet1/0/1] ptp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

On GigabitEthernet 1/0/2, specify IPv4 UDP transport of PTP messages, configure the destination IP address for unicast PTP messages, and enable PTP.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ptp transport-protocol udp
[DeviceB-GigabitEthernet1/0/2] ptp unicast-destination 11.10.10.1
[DeviceB-GigabitEthernet1/0/2] ptp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Specify the IEEE 1588 version 2 PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile 1588v2
```

Specify the BC clock node type.

```
[DeviceC] ptp mode bc
```

Create a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Specify PTP for obtaining the time

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify IPv4 UDP transport of PTP messages, configure the destination IP address for unicast PTP messages, and enable PTP.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ptp transport-protocol udp
[DeviceC-GigabitEthernet1/0/1] ptp unicast-destination 11.10.10.2
[DeviceC-GigabitEthernet1/0/1] ptp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

On GigabitEthernet1/0/2, specify IPv4 UDP transport of PTP messages, configure the destination IP address for unicast PTP messages, and enable PTP.

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ptp transport-protocol udp
[DeviceC-GigabitEthernet1/0/2] ptp unicast-destination 12.10.10.1
[DeviceC-GigabitEthernet1/0/2] ptp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring the base station

Specify PTP domain 0.

Specify IPv4 UDP transport of PTP messages.

Set the destination IP address of unicast PTP messages to 12.10.10.2.

Specify the Request_Response delay measurement mechanism.

For more information, see the configuration guide for the base station.

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.

When the network is stable, perform the following tasks:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief PTP running information for all PTP interfaces.

Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : BC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : ToD0
 ToD direction  : In
 ToD delay time : 1000 (ns)
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 0
Priority2     : 128
Clock quality :
 Class                 : 6
 Accuracy              : 32
 Offset (log variance) : 65535
```

```
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information for all PTP interfaces on Device A.

```
[DeviceA] display ptp interface brief
Name       InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1    0         Master        E2E              Two         0
```

Display PTP clock information on Device B.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : BC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : ToD0
 ToD direction  : In
 ToD delay time : 1000 (ns)
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 0
Priority2     : 128
Clock quality :
 Class                 : 6
 Accuracy              : 32
 Offset (log variance) : 65535
Offset from master : 12 (ns)
Mean path delay    : 323 (ns)
Steps removed      : 1
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information for all PTP interfaces on Device B.

```
[DeviceB] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Slave           E2E              Two         0
GE1/0/2  0         Master          E2E              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 1588 Version 2
PTP mode            : BC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
```

```
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
Offset from master  : 25 (ns)
Mean path delay     : 2791000 (ns)
Steps removed       : 2
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information for all PTP interfaces on Device C.

```
[DeviceC] display ptp interface brief
Name       InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1    0         Slave         E2E              Two         0
GE1/0/2    0         Master        E2E              Two         0
```

Configuration files

- Device A

```
#
 clock protocol ptp
#
 ptp profile IEEE 1588 Version 2
 ptp mode bc
 ptp domain 0
 ptp global enable
 ptp tod0 input delay 1000
 ptp priority clock-source tod0 priority1 0
#
interface GigabitEthernet 1/0/1
 ptp transport-protocol
 ptp unicast-destination 10.10.10.2
 ptp enable
#
```

- Device B

```
#
 clock protocol ptp
#
 ptp profile IEEE 1588 Version 2
 ptp mode bc
 ptp domain 0
 ptp global enable
#
interface GigabitEthernet 1/0/1
 ptp transport-protocol
 ptp unicast-destination 10.10.10.1
 ptp enable
#
```

```
interface GigabitEthernet 1/0/2
 ptp enable
#
```

- Device C

```
#
 clock protocol ptp
#
 ptp profile IEEE 1588 Version 2
 ptp mode bc
 ptp domain 0
 ptp global enable
#
 interface GigabitEthernet 1/0/1
 ptp transport-protocol
 ptp unicast-destination 11.10.10.2
 ptp enable
#
 interface GigabitEthernet 1/0/2
 ptp transport-protocol
 ptp unicast-destination 12.10.10.1
 ptp enable
#
```

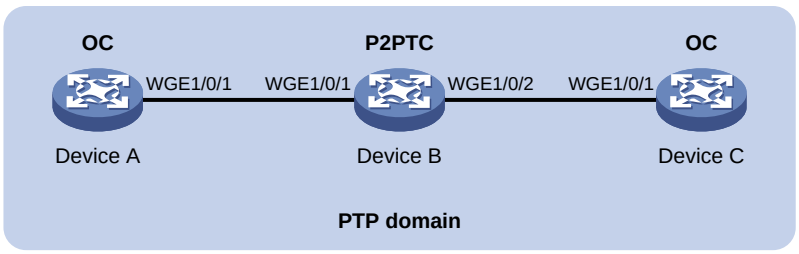
Example: Configuring IEEE 802.1AS PTP

Network configuration

As shown in Figure 1, a PTP domain contains Device A, Device B, and Device C. Configure IEEE 802.1AS PTP as follows for time synchronization:

- Specify the IEEE 802.1AS PTP profile for Device A, Device B, and Device C.
- Specify the OC clock node type for Device A and Device C, and P2PTC clock node type for Device B. These clock nodes elect a GM through BMC based on their respective default GM attributes.
- Use the default peer delay measurement mechanism on all clock nodes in the PTP domain.

Figure 4 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5570S-EI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	Not supported
IE4300-28P-M switch IE4320-28P switch	Not supported
IE4520 series	Not supported
S5135S-EI series	Not supported

Procedures

Configuring Device A

Specify the IEEE 802.1AS PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile 8021as
```

Specify the OC clock node type.

```
[DeviceA] ptp mode oc
```

Specify a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceA] clock protocol ptp
```

Enable PTP on Twenty-FiveGigE 1/0/1.

```
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] ptp enable
[DeviceA-Twenty-FiveGigE1/0/1] quit
```

Configuring Device B

Specify the IEEE 802.1AS PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile 8021as
```

Specify the P2PTC clock node type.

```
[DeviceB] ptp mode p2ptc
```

Specify a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceB] clock protocol ptp
```

Enable PTP on Twenty-FiveGigE 1/0/1.

```
[DeviceB] interface twenty-fivegige 1/0/1
[DeviceB-Twenty-FiveGigE1/0/1] ptp enable
[DeviceB-Twenty-FiveGigE1/0/1] quit
```

Enable PTP on Twenty-FiveGigE 1/0/2.

```
[DeviceB] interface twenty-fivegige 1/0/2
[DeviceB-Twenty-FiveGigE1/0/2] ptp enable
[DeviceB-Twenty-FiveGigE1/0/2] quit
```

Configuring Device C

Specify the IEEE 802.1AS PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile 8021as
```

Specify the OC clock node type.

```
[DeviceC] ptp mode oc
```

Specify a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Specify PTP for obtaining the time.

```
[DeviceC] clock protocol ptp
```

Enable PTP on Twenty-FiveGigE 1/0/1.

```
[DeviceC] interface twenty-fivegige 1/0/1
[DeviceC-Twenty-FiveGigE1/0/1] ptp enable
[DeviceC-Twenty-FiveGigE1/0/1] quit
```

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.

When the network topology is stable, perform the following tasks to verify the PTP configuration:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief information about PTP interfaces.

  # Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 802.1AS
PTP mode            : OC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 246
Priority2     : 248
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 16640
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
```

```
Local clock time   : Sun Jan 15 20:57:29 2011
```

Display brief information about PTP interfaces on Device A.

```
[DeviceA] display ptp interface brief
Name      InstID   State         Delay mechanism  Clock step  Asymmetry correction
WGE1/0/1  0        Master        P2P              Two         0
```

Display PTP clock information on Device B.

```
[DeviceB] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 802.1AS
PTP mode            : P2PTC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 246
Priority2     : 248
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 16640
Offset from master : N/A
Mean path delay    : N/A
Steps removed      : N/A
Local clock time   : Sun Jan 15 20:57:29 2011
```

Display brief information about PTP interfaces on Device B.

```
[DeviceB] display ptp interface brief
Name      InstID    State        Delay mechanism  Clock step  Asymmetry correction
WGE1/0/1   0          N/A           P2P              Two         0
WGE1/0/2   0          N/A           P2P              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : IEEE 802.1AS
PTP mode            : OC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0002
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
```

```
Offset from master : 25 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 2
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device C.

```
[DeviceC] display ptp interface brief
Name      InstID    State        Delay mechanism  Clock step  Asymmetry correction
WGE1/0/1   0         Slave         P2P              Two         0
```

The command outputs show that Device A is elected as the GM and Twenty-FiveGigE 1/0/1 on Device A is the master port.

Configuration files

- Device A and Device C:

```
#
 ptp profile 8021as
 ptp mode oc
 ptp domain 0
 ptp global enable
#
interface Twenty-FiveGigE 1/0/1
 ptp enable
#
```

- Device B

```
#
 ptp profile 8021as
 ptp mode p2ptc
 ptp domain 0
 ptp global enable
#
interface Twenty-FiveGigE 1/0/1
 ptp enable
#
interface Twenty-FiveGigE 1/0/2
 ptp enable
#
```

Example: Configuring SMPTE ST 2059-2 PTP in multicast mode

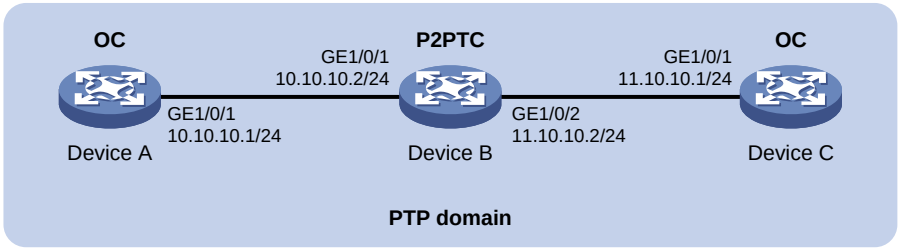
Network configuration

As shown in Figure 5, Device A, Device B, and Device C are in a PTP domain. Configure SMPTE ST 2059-2 PTP in multicast mode as follows for time synchronization:

- Specify the SMPTE ST 2059-2 PTP profile for the devices.
- Configure the multicast PTP transport mode for the devices.

- Specify the OC clock node type for Device A and Device C, and the P2PTC clock node type for Device B. All clock nodes elect a GM through BMC based on their respective default GM attributes.
- Configure the peer delay measurement mechanism (p2p) for Device A and Device C.

Figure 5 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Release 6615Pxx, and Release 6628Pxx
S5570S-EI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, and Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported

Hardware	Software version
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported

Hardware	Software version
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	Not supported
IE4300-28P-M switch IE4320-28P switch	Release 63xx
IE4520 series	Release 66xx
S5135S-EI series	Not supported

Procedures

Configuring Device A

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile st2059-2
```

Specify the OC clock node type.

```
[DeviceA] ptp mode oc
```

Specify a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceA] ptp source 10.10.10.1
```

Specify PTP for obtaining the time.

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify the peer delay measurement mechanism (p2p) and enable PTP.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ptp delay-mechanism p2p
[DeviceA-GigabitEthernet1/0/1] ptp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile st2059-2
```

Specify the P2PTC clock node type.

```
[DeviceB] ptp mode p2ptc
```

Specify a PTP domain.

```
[DeviceB] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceB] ptp source 10.10.10.2
```

Specify PTP for obtaining the time.

```
[DeviceB] clock protocol ptp
```

Enable PTP on GigabitEthernet 1/0/1.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ptp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

Enable PTP on GigabitEthernet 1/0/2.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ptp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile st2059-2
```

Specify the OC clock node type.

```
[DeviceC] ptp mode oc
```

Specify a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Configure the source IP address for multicast PTP transport.

```
[DeviceC] ptp source 11.10.10.1
```

Specify PTP for obtaining the time.

```
[DeviceC] clock protocol ptp
```

On GigabitEthernet 1/0/1, specify the peer delay measurement mechanism (p2p) and enable PTP.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ptp delay-mechanism p2p
[DeviceC-GigabitEthernet1/0/1] ptp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the

S6550XE-HI switch series and S6525XE-HI switch series.

When the network topology is stable, perform the following tasks to verify the PTP configuration:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief information about PTP interfaces.

  # Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : OC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

  # Display brief information about PTP interfaces on Device A.

```
[DeviceA] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Master        P2P              Two         0
```

  # Display PTP clock information on Device B.

```
[DeviceB] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : P2PTC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
```

```
Offset from master : N/A
Mean path delay    : N/A
Steps removed      : N/A
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device B.

```
[DeviceB] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         N/A           P2P              Two         0
GE1/0/2  0         N/A           P2P              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : OC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0002
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                : 248
 Accuracy             : 254
 Offset (log variance) : 65535
Offset from master : 25 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 2
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief information about PTP interfaces on Device C.

```
[DeviceC] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Slave         P2P              Two         0
```

The output shows that Device A is elected as the GM and GigabitEthernet1/0/1 on Device A is the master port.

Configuration files

- Device A:

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode oc
 ptp domain 0
 ptp global enable
 ptp source 10.10.10.1
```

```
#
interface GigabitEthernet 1/0/1
 ptp delay-mechanism p2p
 ptp enable
#
```

- Device B:

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode p2ptc
 ptp domain 0
 ptp global enable
 ptp source 10.10.10.2
#
interface GigabitEthernet 1/0/1
 ptp enable
#
interface GigabitEthernet 1/0/2
 ptp enable
#
```

- Device C:

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode oc
 ptp domain 0
 ptp global enable
 ptp source 11.10.10.1
#
interface GigabitEthernet 1/0/1
 ptp delay-mechanism p2p
 ptp enable
#
```

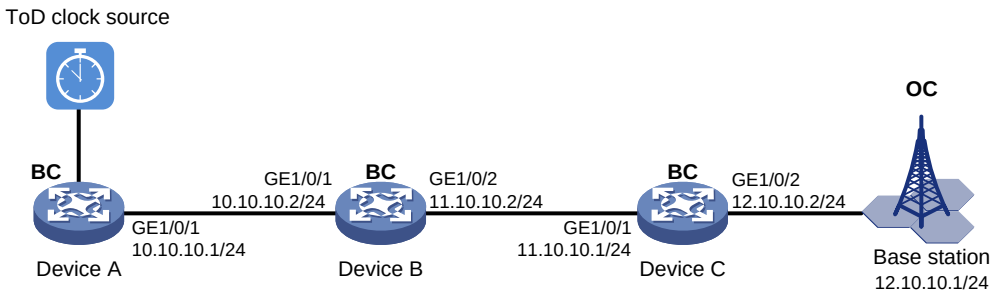
Example: Configuring PTP (SMPTE ST 2059-2, IPv4 UDP transport, unicast transmission)

Network configuration

As shown in Figure 6, configure PTP (SMPTE ST 2059-2, IPv4 UDP transport, unicast transmission) to enable Device A, Device B, Device C, and the base station to synchronize time with the ToD clock source.

- Specify the SMPTE ST 2059-2 PTP profile and unicast IPv4 UDP transport of PTP messages for Device A, Device B, and Device C.
- Assign Device A, Device B, Device C, and the base station to PTP domain 0. Specify the BC clock node type for Device A, Device B, and Device C.
- Connect Device A to the ToD clock source and Device C to the base station.
- Use the default Request_Response delay measurement mechanism on all clock nodes in the PTP domain.

Figure 6 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, and Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later versions, and Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Release 6615Pxx, and Release 6628Pxx
S5500V2-EI switch series	Not supported
MS4520V2-30F	Not supported
MS4520V2-30C MS4520V2-54C	Not supported
MS4520V2-28S MS4520V2-24TP	Not supported
ES5500 switch series	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, and Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, and Release 6628Pxx

S5000-EI switch series	Release 6615Pxx, and Release 6628Pxx
MS4600 switch series	Release 6615Pxx, and Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported

WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M switch series (except the IE4300-28P-M) IE4320 switch series (except the IE4320-28P)	Not supported
IE4300-28P-M IE4320-28P	Not supported
IE4520 series	Not supported
S5135S-EI series	Not supported

Procedures

IMPORTANT:

The SMPTE ST 2059-2 PTP profile supports IPv4 UDP transport rather than IEEE 802.3/Ethernet transport of PTP messages. It supports both multicast and unicast transmission of PTP messages.

IMPORTANT:

The device does not provide ToD interfaces. It can be deployed as Device B or Device C but not Device A.

Before configuration, assign IP addresses to the interfaces, and make sure the devices can reach each other. (Details not shown.)

Configuring Device A

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceA> system-view
[DeviceA] ptp profile st2059-2
```

Specify the BC clock node type.

```
[DeviceA] ptp mode bc
```

Create a PTP domain.

```
[DeviceA] ptp domain 0
```

Enable PTP globally.

```
[DeviceA] ptp global enable
```

Configure the device to use ToD 0 to receive clock signals and set the receive delay correction to 1000 nanoseconds

```
[DeviceA] ptp tod0 input delay 1000
```

Set priority 1 to **0** for the ToD 0 clock.

```
[DeviceA] ptp priority clock-source tod0 priority1 0
```

On GigabitEthernet 1/0/1, configure the destination IP address for unicast PTP messages and enable PTP. (The SMPTE ST 2059-2 PTP profile transports PTP messages over IPv4 UDP by default.)

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ptp unicast-destination 10.10.10.2
[DeviceA-GigabitEthernet1/0/1] ptp enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceB> system-view
[DeviceB] ptp profile st2059-2
```

Specify the BC clock node type.

```
[DeviceB] ptp mode bc
```

Create a PTP domain.

```
[DeviceB] ptp domain 0
```

Enable PTP globally.

```
[DeviceB] ptp global enable
```

Specify PTP for obtaining the time

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, configure the destination IP address for unicast PTP messages and enable PTP. (The SMPTE ST 2059-2 PTP profile transports PTP messages over IPv4 UDP by default.)

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ptp unicast-destination 10.10.10.1
[DeviceB-GigabitEthernet1/0/1] ptp enable
[DeviceB-GigabitEthernet1/0/1] quit
```

On GigabitEthernet 1/0/2, configure the destination IP address for unicast PTP messages and enable PTP. (The SMPTE ST 2059-2 PTP profile transports PTP messages over IPv4 UDP by default.)

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ptp unicast-destination 11.10.10.1
[DeviceB-GigabitEthernet1/0/2] ptp enable
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C

Specify the SMPTE ST 2059-2 PTP profile.

```
<DeviceC> system-view
[DeviceC] ptp profile st2059-2
```

Specify the BC clock node type.

```
[DeviceC] ptp mode bc
```

Create a PTP domain.

```
[DeviceC] ptp domain 0
```

Enable PTP globally.

```
[DeviceC] ptp global enable
```

Specify PTP for obtaining the time

```
[DeviceA] clock protocol ptp
```

On GigabitEthernet 1/0/1, configure the destination IP address for unicast PTP messages and enable PTP.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ptp unicast-destination 11.10.10.2
[DeviceC-GigabitEthernet1/0/1] ptp enable
[DeviceC-GigabitEthernet1/0/1] quit
```

On GigabitEthernet1/0/2, configure the destination IP address for unicast PTP messages and enable PTP. (The SMPTE ST 2059-2 PTP profile transports PTP messages over IPv4 UDP by default.)

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ptp unicast-destination 12.10.10.1
[DeviceC-GigabitEthernet1/0/2] ptp enable
[DeviceC-GigabitEthernet1/0/2] quit
```

Configuring the base station

Specify PTP domain 0.

Specify IPv4 UDP transport of PTP messages.

Set the destination IP address of unicast PTP messages to 12.10.10.2.

Specify the Request_Response delay measurement mechanism.

For more information, see the configuration guide for the base station.

Verifying the configuration

IMPORTANT:

- The **Lock status** field in the output from the **display ptp clock** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.
- The **InstID** field in the output from the **display ptp interface brief** command is available only for the S6550XE-HI switch series and S6525XE-HI switch series.

When the network is stable, perform the following tasks to verify the PTP configuration:

- Use the **display ptp clock** command to display PTP clock information.
- Use the **display ptp interface brief** command to display brief PTP running information.

Display PTP clock information on Device A.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : BC
Slave only          : No
Lock status         : Unlocked
Clock ID            : 000FE2-FFFE-FF0000
Clock type          : ToD0
 ToD direction  : In
 ToD delay time : 1000 (ns)
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 0
```

```
Priority2     : 128
Clock quality :
 Class                : 6
 Accuracy             : 32
 Offset (log variance) : 65535
Offset from master : 0 (ns)
Mean path delay    : 0 (ns)
Steps removed      : 0
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information on Device A.

```
[DeviceA] display ptp interface brief
Name       InstID        State        Delay mechanism  Clock step  Asymmetry correction
GE1/0/1    0               Master       E2E              Two         0
```

Display PTP clock information on Device B.

```
[DeviceA] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : BC
Slave only          : No
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0001
Clock type          : ToD0
 ToD direction  : In
 ToD delay time : 1000 (ns)
Clock domain        : 0
Number of PTP ports : 1
Priority1     : 0
Priority2     : 128
Clock quality :
 Class                : 6
 Accuracy             : 32
 Offset (log variance) : 65535
Offset from master : 12 (ns)
Mean path delay    : 323 (ns)
Steps removed      : 1
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information on Device B.

```
[DeviceB] display ptp interface brief
Name     InstID    State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1  0         Slave         E2E              Two         0
GE1/0/2  0         Master        E2E              Two         0
```

Display PTP clock information on Device C.

```
[DeviceC] display ptp clock
PTP global state    : Enabled
PTP profile         : SMPTE ST 2059-2
PTP mode            : BC
Slave only          : No
```

```
Lock status         : Locked
Clock ID            : 000FE2-FFFE-FF0002
Clock type          : Local
Clock domain        : 0
Number of PTP ports : 2
Priority1     : 128
Priority2     : 128
Clock quality :
 Class                 : 248
 Accuracy              : 254
 Offset (log variance) : 65535
Offset from master  : 25 (ns)
Mean path delay     : 323 (ns)
Steps removed       : 2
Local clock time   : Sun Jan 15 20:57:29 2019
```

Display brief PTP running information on Device C.

```
[DeviceC] display ptp interface brief
Name        InstID      State         Delay mechanism  Clock step  Asymmetry correction
GE1/0/1     0           Slave           E2E              Two         0
GE1/0/2     0           Master          E2E              Two         0
```

Configuration files

- Device A

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode bc
 ptp domain 0
 ptp global enable
 ptp tod0 input delay 1000
 ptp priority clock-source tod0 priority1 0
#
interface GigabitEthernet 1/0/1
 ptp unicast-destination 10.10.10.2
 ptp enable
#
```

- Device B

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode bc
 ptp domain 0
 ptp global enable
#
interface GigabitEthernet 1/0/1
```

```
 ptp unicast-destination 10.10.10.1
 ptp enable
#
interface GigabitEthernet 1/0/2
 ptp enable
#
```

- Device C

```
#
 clock protocol ptp
#
 ptp profile st2059-2
 ptp mode bc
 ptp domain 0
 ptp global enable
#
interface GigabitEthernet 1/0/1
 ptp unicast-destination 11.10.10.2
 ptp enable
#
 interface GigabitEthernet 1/0/2
 ptp unicast-destination 12.10.10.1
 ptp enable
#
```

Contents

Introduction

This document provides configuration examples for using simple multichassis link aggregation (S-MLAG).

S-MLAG enhances dynamic link aggregation to establish an aggregation that spans multiple standalone devices to a remote device.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

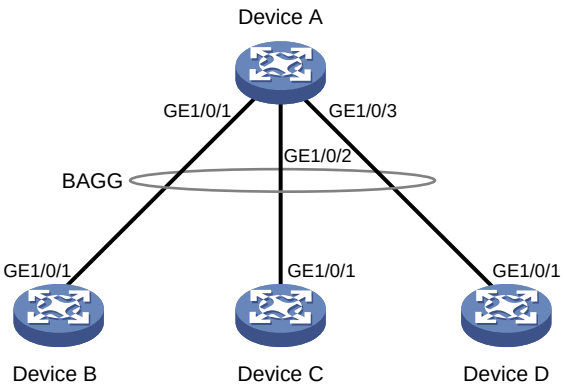
The following information is provided based on the assumption that you have basic knowledge of S-MLAG.

Example: Configuring S-MLAG

Network configuration

Device B, Device C, and Device D are standalone devices. As shown in Figure 1, configure Device B, Device C, and Device D as S-MLAG devices to establish a multidevice aggregate link with Device A.

Figure 1 Network diagram



Analysis

To establish a multidevice aggregate link with Device A, you must perform the following tasks on Device B, Device C, and Device D:

1. Create a Layer 2 dynamic aggregate interface and assign GigabitEthernet 1/0/1 to its aggregation group.
2. Assign the aggregate interfaces to the same DR group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 63xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

Before you assign an interface to an aggregation group, use the **display this** command in interface view to identify whether attribute settings exist, including port isolation, QinQ, VLAN, and VLAN mapping settings. If attribute settings exist, use the corresponding **undo** commands to remove them.

Configure the link aggregation settings other than S-MLAG settings on each S-MLAG device. Make sure the settings are consistent across the S-MLAG devices.

As a best practice, maintain consistency across S-MLAG devices in service feature configuration.

Procedures

Configuring Device A

Create Layer 2 aggregate interface Bridge-Aggregation 10, and set the link aggregation mode to dynamic.

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 10
[DeviceA-Bridge-Aggregation10] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation10] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to aggregation group 10.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 10
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 10
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 10
[DeviceA-GigabitEthernet1/0/3] quit
```

Configuring Device B

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceB> system-view
[DeviceB] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceB] lacp system-priority 123
```

Set the LACP system number to 1.

```
[DeviceB] lacp system-number 1
```

Create Layer 2 aggregate interface Bridge-Aggregation 2, and set the link aggregation mode to dynamic.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] link-aggregation mode dynamic
```

Assign Bridge-Aggregation 2 to S-MLAG group 100.

```
[DeviceB-Bridge-Aggregation2] port s-mlag group 100
```

```
[DeviceB-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 2.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configuring Device C

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceC> system-view
[DeviceC] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceC] lacp system-priority 123
```

Set the LACP system number to 2.

```
[DeviceC] lacp system-number 2
```

Create Layer 2 aggregate interface Bridge-Aggregation 3, and set the link aggregation mode to dynamic.

```
[DeviceC] interface bridge-aggregation 3
[DeviceC-Bridge-Aggregation3] link-aggregation mode dynamic
```

Assign Bridge-Aggregation 3 to S-MLAG group 100.

```
[DeviceC-Bridge-Aggregation3] port s-mlag group 100
```

Assign GigabitEthernet 1/0/1 to aggregation group 3.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceC-GigabitEthernet1/0/1] quit
```

Configuring Device D

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceD> system-view
[DeviceD] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceD] lacp system-priority 123
```

Set the LACP system number to 3.

```
[DeviceD] lacp system-number 3
```

Create Layer 2 aggregate interface Bridge-Aggregation 4, and set the link aggregation mode to dynamic.

```
[DeviceD] interface bridge-aggregation 4
[DeviceD-Bridge-Aggregation4] link-aggregation mode dynamic
```

Assign Bridge-Aggregation 4 to S-MLAG group 100.

```
[DeviceD-Bridge-Aggregation4] port s-mlag group 100
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[DeviceD] interface gigabitethernet 1/0/1
[DeviceD-GigabitEthernet1/0/1] port link-aggregation group 4
[DeviceD-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 on Device A are Selected ports.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation10
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, a0c7-9afd-0100
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
  GE1/0/3             S        32768    3        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16385    50100    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    32769    50100    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/3             32768    49153    50100    0x7b  , 0001-0001-0001 {ACDEF}
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
interface Bridge-Aggregation10
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 10
```

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 10
#
```

- Device B:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 1
 lacp system-priority 123
#
interface Bridge-Aggregation2
 link-aggregation mode dynamic
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 2
#
```

- Device C:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 2
 lacp system-priority 123
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 3
#
```

- Device D:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 3
 lacp system-priority 123
#
interface Bridge-Aggregation4
 link-aggregation mode dynamic
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 combo enable fiber
 port link-aggregation group 4
#
```

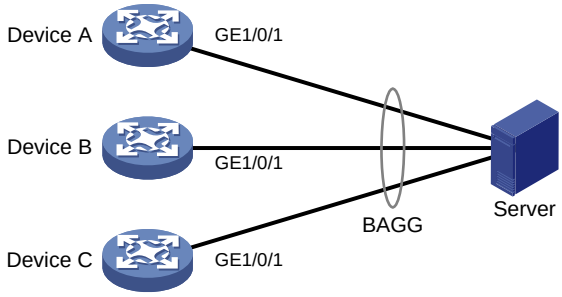
Example: Aggregating server-side links by using S-MLAG

Network configuration

As shown in Figure 2, configure S-MLAG as follows:

- Connect GigabitEthernet 1/0/1 interfaces on Device A, Device B, and Device C to the server, and configure S-MLAG to aggregate the links to the server.
- Configure the server-facing aggregate interfaces on Device A, Device B, and Device C as edge aggregate interfaces for the aggregation member ports to forward traffic correctly before link aggregation is set up on the server.

Figure 2 Network diagram



Analysis

To create a multichassis aggregate link on Device A, Device B, and Device C, perform the following tasks:

- Create server-facing Layer 2 dynamic aggregate interfaces.
- Assign the aggregate interfaces to an S-MLAG group.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx

S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx

S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure S-MLAG, follow these restrictions and guidelines:

- When you assign a port to an aggregation group, the recommended configuration procedure is as follows:
  a. Use the **`display this`** command in interface view to check the following attribute configurations of the port:
  - Port isolation.
  - QinQ.
  - VLAN.
  - VLAN mapping.

b. If any of the above configurations exist, use the **undo** forms of the corresponding commands to remove these configurations. This enables the port to use the default attribute configurations.

c. Assign the port to the aggregation group.

- Make sure the S-MLAG member devices have consistent link aggregation configuration.
- To ensure correct service traffic forwarding, configure the same service settings on the S-MLAG member devices.

Procedures

Configuring Device A

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceA> system-view
[DeviceA] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceA] lacp system-priority 123
```

Set the LACP system number to 1.

```
[DeviceA] lacp system-number 1
```

Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
```

Configure Bridge-Aggregation 1 as an edge aggregate interface.

```
[DeviceA-Bridge-Aggregation1] lacp edge-port
```

Assign Bridge-Aggregation 1 to S-MLAG group 100.

```
[DeviceA-Bridge-Aggregation1] port s-mlag group 100
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
```

Configuring Device B

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceB> system-view
[DeviceB] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceB] lacp system-priority 123
```

Set the LACP system number to 2.

```
[DeviceB] lacp system-number 2
```

Create Layer 2 aggregate interface Bridge-Aggregation 2, and set the link aggregation mode to dynamic.

```
[DeviceB] interface bridge-aggregation 2
[DeviceC-Bridge-Aggregation2] link-aggregation mode dynamic
```

Configure Bridge-Aggregation 2 as an edge aggregate interface.

```
[DeviceB-Bridge-Aggregation2] lacp edge-port
```

Assign Bridge-Aggregation 2 to S-MLAG group 100.

```
[DeviceB-Bridge-Aggregation2] port s-mlag group 100
```

Assign GigabitEthernet 1/0/1 to aggregation group 2.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/1] quit
```

Configuring Device C

Set the LACP system MAC address to 0001-0001-0001.

```
<DeviceC> system-view
[DeviceC] lacp system-mac 1-1-1
```

Set the LACP system priority to 123.

```
[DeviceC] lacp system-priority 123
```

Set the LACP system number to 3.

```
[DeviceC] lacp system-number 3
```

Create Layer 2 aggregate interface Bridge-Aggregation 3, and set the link aggregation mode to dynamic.

```
[DeviceC] interface bridge-aggregation 3
[DeviceC-Bridge-Aggregation3] link-aggregation mode dynamic
```

Configure Bridge-Aggregation 3 as an edge aggregate interface.

```
[DeviceC-Bridge-Aggregation3] lacp edge-port
```

Assign Bridge-Aggregation 3 to S-MLAG group 100.

```
[DeviceC-Bridge-Aggregation3] port s-mlag group 100
```

Assign GigabitEthernet 1/0/1 to aggregation group 3.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Before you configure dynamic link aggregation on the server, verify that the aggregation member ports are in individual state on Device A, Device B, and Device C to forward traffic independently.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
```

```
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port               Status   Priority Index    Oper-Key               Flag
  GE1/0/1            I        32768    16385    50100                  {AG}
Remote:
  Actor              Priority Index    Oper-Key SystemID               Flag
  GE1/0/1            32768    0        0        0x8000, 0000-0000-0000 {DEF}
[DeviceB] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port               Status   Priority Index    Oper-Key               Flag
  GE1/0/1            I        32768    32769    50100                  {AG}
Remote:
  Actor              Priority Index    Oper-Key SystemID               Flag
  GE1/0/1            32768    0        0        0x8000, 0000-0000-0000 {DEF}
[DeviceC] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation3
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port               Status   Priority Index    Oper-Key               Flag
  GE1/0/1            I        32768    49153    50100                  {AG}
Remote:
  Actor              Priority Index    Oper-Key SystemID               Flag
```

```
  GE1/0/1             32768    0        0        0x8000, 0000-0000-0000 {DEF}
```

After you configure dynamic link aggregation on the server, verify that the aggregation member ports are selected on Device A, Device B, and Device C, which indicates that the multichassis link aggregation has been set up.

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    16385    50100                  {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    1        1        0x8000, 5022-e533-0400 {ACDEF}
[DeviceB] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    32769    50100                  {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    2        1        0x8000, 5022-e533-0400 {ACDEF}
[DeviceC] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
```

```
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation3
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1(R)          S        32768    49153    50100                  {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1             32768    3        1        0x8000, 5022-e533-0400 {ACDEF}
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Device A:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 1
 lacp system-priority 123
#
interface Bridge-Aggregation1
 link-aggregation mode dynamic
 lacp edge-port
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-aggregation group 1
#
```

- Device B:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 2
 lacp system-priority 123
#
interface Bridge-Aggregation2
 link-aggregation mode dynamic
 lacp edge-port
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-aggregation group 2
#
```

- Device C:

```
#
 lacp system-mac 0001-0001-0001
 lacp system-number 3
 lacp system-priority 123
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 lacp edge-port
 port s-mlag group 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-aggregation group 3
#
```

Contents

Introduction

This document provides Puppet configuration examples.

Puppet is an open-source configuration management tool. It provides the Puppet language. You can use the Puppet language to create configuration manifests and save them to a server. You can then use the server for centralized configuration enforcement and management.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

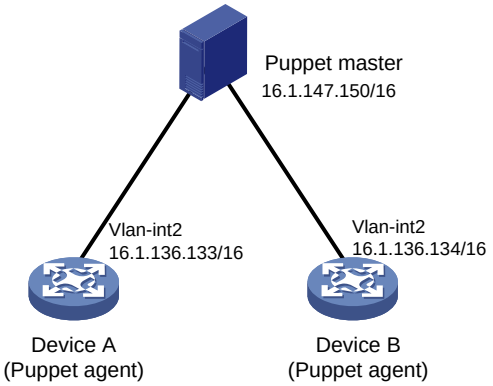
This document assumes that you have basic knowledge of Puppet.

Example: Configuring Puppet

Network configuration

As shown in Figure 1, Puppet agents Device A and Device B are connected to the Puppet master. Use Puppet to create VLAN 100 on each Puppet agent.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported

Hardware	Software version
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported

Hardware	Software version
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring the Puppet master

1. Assign an IP address to the Puppet master. (Details not shown.)
2. Install Puppet on the Puppet master.
   ```
   $ sudo apt-get install puppetmaster
   ```
3. Verify that Puppet configuration file **puppet.conf** is created in directory **/etc/puppet**.
   If the file does not exist, execute the following command to create the file:
   ```
   $ sudo puppet master –genconfig > puppet.conf
   ```
4. Add files provided by H3C:

Copy the type and provider library files to directory **/etc/puppet/modules/custom/lib/puppet**. If conflicts exist, overwrite the existing files. (Details not shown.)

Create directory **manifests/nodes** in directory **/etc/puppet/**.

```
$ sudo mkdir –p /etc/puppet/manifests/nodes
```

Copy H3C file **puppet.master.com.pp** to directory **/etc/puppet/manifests/nodes/**. (Details not shown.)

5. Configure file **site.pp**:

Go to directory **/etc/puppet/manifests/** and create file **site.pp** in the directory.

```
$ cd ..
$ sudo touch site.pp
```

Edit file **site.pp**.

```
node '16.1.136.133'{
  netdev_device{'device':
    ensure => undo_shutdown,
    username => 'test',
    password => 'test',
    ipaddr => '16.1.136.133',
    }
    include custom
}
node '16.1.136.134'{
  netdev_device{'device':
    ensure => undo_shutdown,
    username => 'test',
    password => 'test',
    ipaddr => '16.1.136.134',
    }
    include custom
}
```

6. Configure file **init.pp**:

Create directory **modules/custom/manifests** in directory **/etc/puppet/** to store configuration manifests.

```
$ sudo mkdir -p /etc/puppet/modules/custom/manifests
```

Create configuration manifest **init.pp** in directory **/etc/puppet/modules/custom/manifests**.

```
$ sudo touch init.pp
```

Edit file **init.pp**.

```
class custom{
  netdev_vlan{'vlan100':
    ensure => undo_shutdown,
    id => 100,
    require => Netdev_device['device'],
    }
}
```

Configuring Puppet agent Device A

1. Assign an IP address to Device A. (Details not shown.)

```
<DeviceA> system-view
[DeviceA] interface vlan-interface 2
```

```
[DeviceA-Vlan-interface2] ip address 16.1.136.133 255.255.0.0
[DeviceA-Vlan-interface2] quit
```

2. Configure the device as the NETCONF over SSH server:

   # Generate RSA key pairs. Leave the key pair to use the default key pair name.

   ```
   [DeviceA] public-key local create rsa
   ```

   # Enable NETCONF over SSH.

   ```
   [DeviceA] netconf ssh server enable
   ```

   # Enable scheme authentication for NETCONF over SSH users.

   ```
   [DeviceA] line vty 0 63
   [DeviceA-line-vty0-63] authentication-mode scheme
   [DeviceA-line-vty0-63] quit
   ```

   # Create device management user **test**. Set the password to **test**, and assign the SSH service and network-admin user role to the user.

   ```
   [DeviceA] local-user test class manage
   [DeviceA-luser-manage-test] password simple test
   [DeviceA-luser-manage-test] service-type ssh
   [DeviceA-luser-manage-test] authorization-attribute user-role network-admin
   [DeviceA-luser-manage-test] quit
   ```

3. Configure the device as an NTP client to synchronize its system time to the system time on the Puppet master:

   # Enable the NTP service

   ```
   [DeviceA] ntp-service enable
   ```

   # Configure the device to use NTP to obtain the UTC time.

   ```
   [DeviceA] clock protocol ntp
   ```

   # Configure the device to operate in NTP broadcast client mode and use VLAN-interface 2 to receive NTP broadcast packets.

   ```
   [DeviceA] interface vlan-interface 2
   [DeviceA-Vlan-interface2] ntp-service broadcast-client
   [DeviceA-Vlan-interface2] quit
   ```

4. Start Puppet on the device.

   ```
   [DeviceA] third-part-process start name puppet arg agent --certname=16.1.136.133
   --server=16.1.147.150
   ```

   The device will act as a Puppet client to request a certificate from the Puppet master.

Configuring Puppet agent Device B

The steps are similar to the steps for Device A

Using the Puppet master to issue certificates to the Puppet clients

Use the **`puppet cert list`** command to display devices that require a certificate. (Details not shown.)

Sign a certificate for Device A.

```
$ sudo puppet cert sign 16.1.136.133
```

After Device A obtains a certificate, it obtains a configuration manifest from the Puppet master and run the manifest.

Sign a certificate for Device B. (Details not shown.)

Verifying the configuration

Display device configuration information. VLAN 100 is created. (Details not shown.)

Configuration files

- Puppet master:
  The type and provider library files and the **puppet.master.com.pp** file are provided by H3C.
- Device A:

```
#
 clock protocol ntp
#
interface Vlan-interface2
 ip address 16.1.136.133 255.255.0.0
 ntp-service broadcast-client
#
 ntp-service enable
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 idle-timeout 0 0
#
local-user test class manage
 password hash $h$6$x0kIJnaHZkFFa3Ga$H4yMQnG96xjHiTID+6UPyJrTLXru6RJaGqrCKpxmo2O
KUVWujeoTcDEovLt6LzKIUyN7J3i5Tq2rOQPdj2Nrww==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 netconf ssh server enable
#
```

Contents

Introduction

The following information provides examples for configuring 802.1X authentication to ensure network access security.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

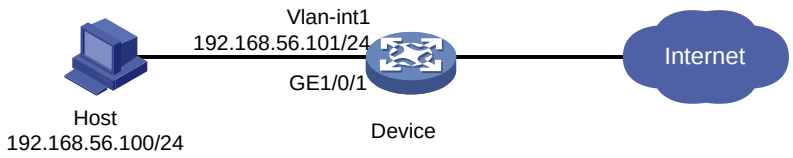
The following information is provided based on the assumption that you have basic knowledge of 802.1X.

Example: Configuring local 802.1X authentication

Network configuration

As shown in Figure 1, the device performs local 802.1X authentication on GigabitEthernet 1/0/1 to control Internet access of users. The interface performs port-based access control for 802.1X authentication.

Figure 1 Network diagram



Analysis

For the device to authenticate the 802.1X user on the host, add the 802.1X username and password to the device.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the	Release 63xx

Hardware	Software version
S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

As a best practice to avoid valid users from being blocked, do not enable 802.1X globally before you finish all settings.

802.1X settings take effect on an interface only when 802.1X is enabled both globally and on the interface.

Procedures

Configuring the device

1. Configure a local user:

   # Add a network access user named **dot1x** and enter its view.

   ```
   <Device> system-view
   [Device] local-user dot1x class network
   New local user added.
   ```

   # Set the user password to **123456TESTplat&!** in plaintext form.

   ```
   [Device-luser-network-dot1x] password simple 123456TESTplat&!
   ```

   # Allow the user to use the LAN access service.

   ```
   [Device-luser-network-dot1x] service-type lan-access
   [Device-luser-network-dot1x] quit
   ```

2. Create VLAN-interface 1 and assign an IP address to the VLAN interface. The VLAN interface will be the gateway of the host.

   ```
   [Device] interface vlan-interface 1
   [Device-Vlan-interface1] ip address 192.168.56.101 255.255.255.0
   [Device-Vlan-interface1] quit
   ```

3. Configure 802.1X authentication:

   # Enable 802.1X on interface GigabitEthernet 1/0/1.

   ```
   [Device] interface gigabitethernet1/0/1
   [Device-GigabitEthernet1/0/1] dot1x
   ```

   # Enable port-based access control.

   ```
   [Device-GigabitEthernet1/0/1] dot1x port-method portbased
   [Device-GigabitEthernet1/0/1] quit
   ```

   # Enable 802.1X globally.

   ```
   [Device] dot1x
   ```

Configuring the 802.1X client

Restrictions and guidelines

This example uses iNode PC 7.3 (E0518) to describe the procedure.

If the host runs the Windows XP built-in 802.1X client, configure the network connection properties as follows:

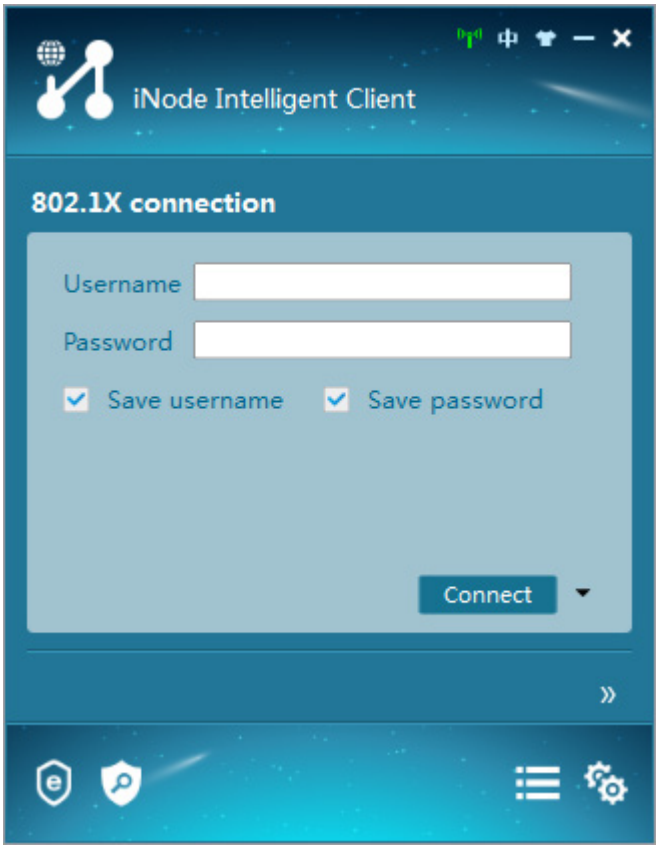
1. Click the **Authentication** tab of the properties window.
2. Select the **Enable IEEE 802.1X authentication for this network** option.
3. Select MD5 challenge as the EAP type.
4. Click **OK**.

Make sure the client can update its IP address to access the resources in the authorized VLAN after passing authentication.

Procedure

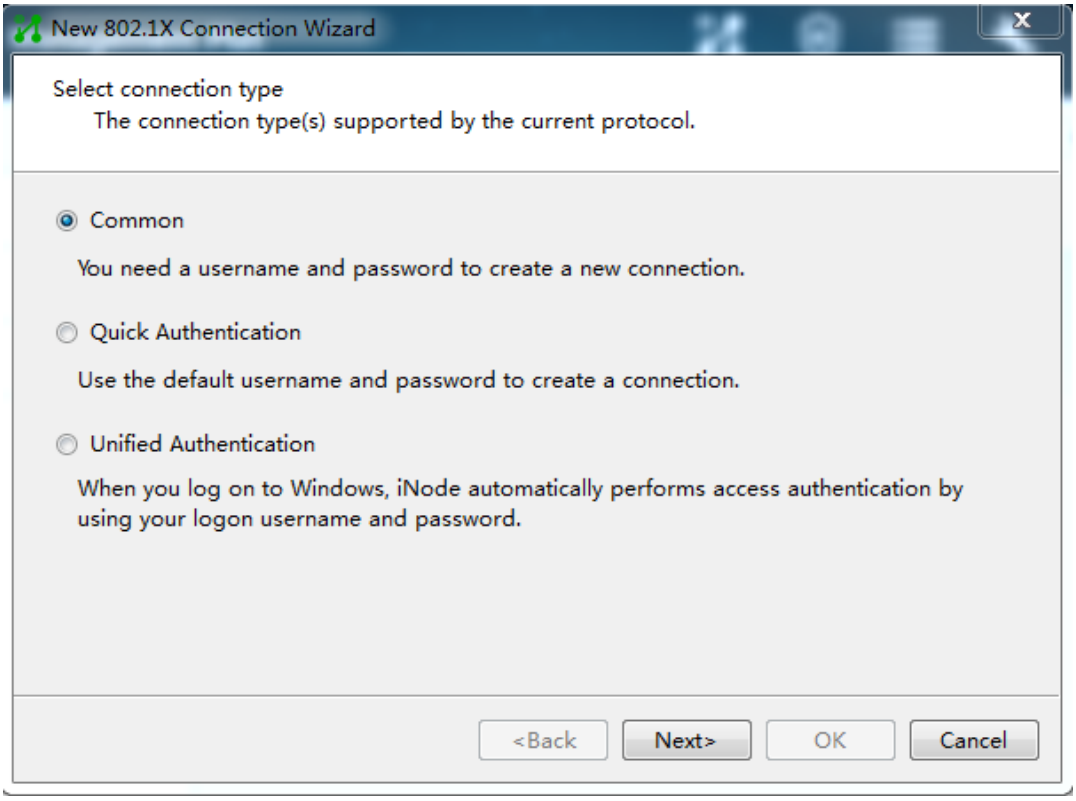
1. Run the iNode client.

Figure 2 iNode client



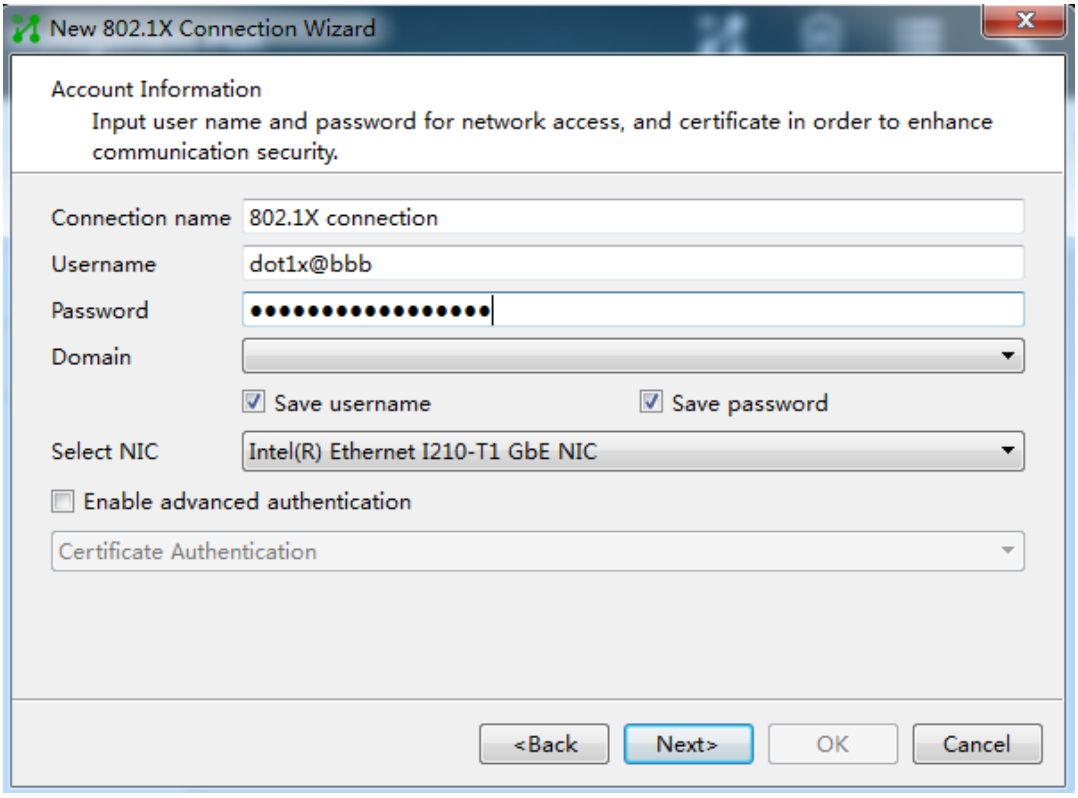
2. Create a new 802.1X connection.
3. On the **New 802.1X Connection Wizard** window, select **Common**, and then click **Next**.

Figure 3 Creating an 802.1X connection



4. Enter the 802.1X connection name, username, and password, and then click **Next**.

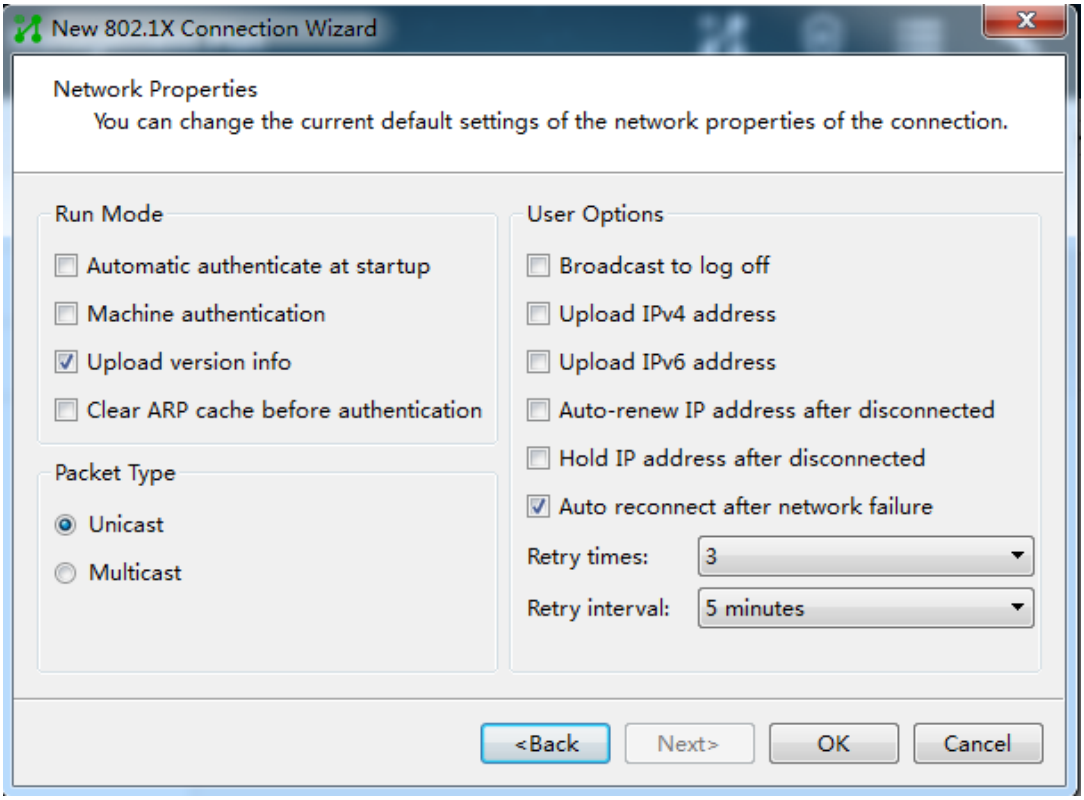
Figure 4 Configuring the 802.1X connection name, username, and password



5. Configure the network property settings, and then click **OK**.

   Do not select **Upload version info** in the **Run Mode** area. The device cannot recognize the version number in EAP packets.

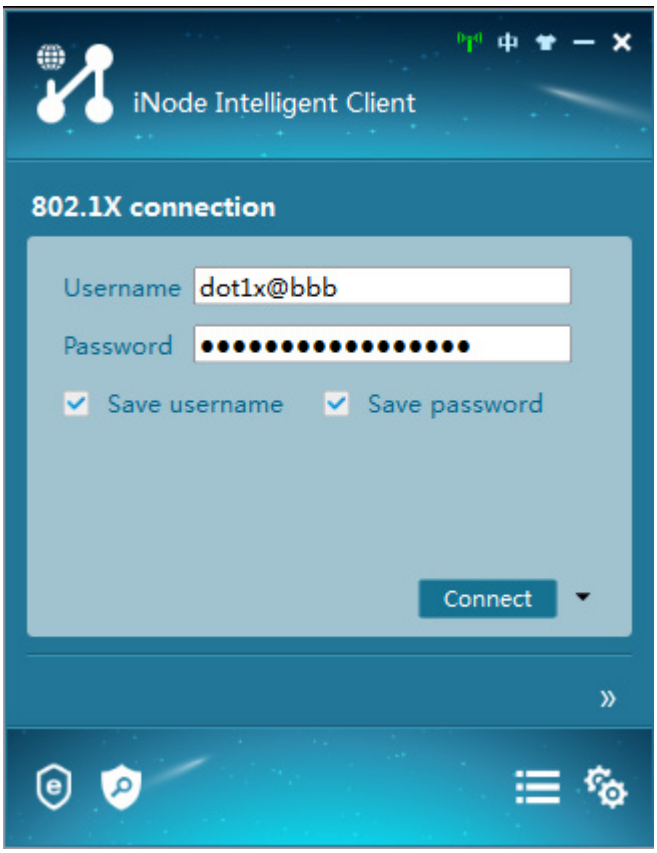
   Figure 5 Configuring 802.1X connection properties



6. Initiate the 802.1X connection.

   Enter the username and password on the iNode client, and then click **Connect**.

Figure 6 Initiating the 802.1X connection



Verifying the configuration

IMPORTANT:

Support for VSI-related fields depends on the device model.

Display 802.1X information on interface GigabitEthernet 1/0/1.

```
[Device] display dot1x interface gigabitethernet 1/0/1
 Global 802.1X parameters:
   802.1X authentication                : Enabled
   CHAP authentication                  : Enabled
   Max-tx period                        : 30 s
   Handshake period                     : 15 s
   Offline detect period                : 300 s
   Quiet timer                          : Disabled
       Quiet period                     : 60 s
   Supp timeout                         : 30 s
   Server timeout                       : 100 s
   Reauth period                        : 3600 s
   Max auth requests                    : 2
   User aging period for Auth-Fail VLAN : 1000 s
   User aging period for Auth-Fail VSI  : 1000 s
   User aging period for critical VLAN  : 1000 s
```

```
  User aging period for critical VSI   : 1000 s
  User aging period for guest VLAN     : 1000 s
  User aging period for guest VSI      : 1000 s
  EAD assistant function               : Disabled
      EAD timeout                      : 30 min
  Domain delimiter                     : @
Online 802.1X wired users              : 0
GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : Port-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : Not configured
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  Guest VSI                        : Not configured
  Auth-Fail VSI                    : Not configured
  Critical VSI                     : Not configured
  Add Guest VSI delay              : Disabled
  User aging                       : Enabled
  Server-recovery online-user-sync : Disabled
  Auth-Fail EAPOL                  : Disabled
  Critical EAPOL                   : Disabled
  Discard duplicate EAPOL-Start    : No

  EAPOL packets: Tx 0, Rx 0
  Sent EAP Request/Identity packets : 0
       EAP Request/Challenge packets: 0
       EAP Success packets: 0
       EAP Failure packets: 0
  Received EAPOL Start packets : 0
           EAPOL LogOff packets: 0
           EAP Response/Identity packets : 0
```

```
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 0
```

After the user passes authentication, display online 802.1X user information.

```
[Device] display dot1x connection
```

Configuration files

```
#
interface Vlan-interface1
 ip address 192.168.56.101 255.255.255.0
#
local-user localuser class network
 password cipher $c$3$YPkufRcxFR3KdpUCHFiNkns/YFPmbJkG/pQxBg==
 service-type lan-access
 authorization-attribute user-role network-operator
#
interface GigabitEthernet1/0/1
 dot1x
 dot1x port-method portbased
#
dot1x
#
```

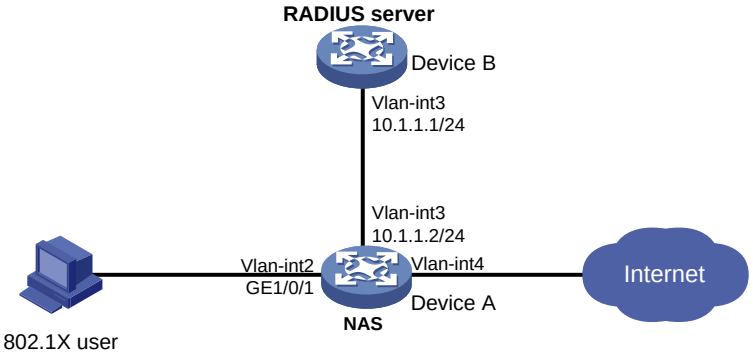
Example: Configuring RADIUS-based 802.1X authentication (an H3C device acts as the RADIUS server)

Network configuration

As shown in Figure 7, Device B acts as the RADIUS server to provide authentication and authorization services for the 802.1X user connected to Device A (the NAS).

After the user passes authentication, the RADIUS server assigns VLAN 4 to GigabitEthernet 1/0/1 (the NAS port that the user is connecting to).

Figure 7 Network diagram



Analysis

- For the RADIUS server to authenticate the 802.1X user, perform the following tasks on the RADIUS server:
  - **a.** Add the device to the RADIUS server as a RADIUS client.
  - **b.** Add the 802.1X username and password to the RADIUS server.
- For the user to access resources in VLAN 4 after it passes authentication, specify VLAN 4 as the authorization VLAN for the user on the RADIUS server.
- To ensure secure transmission between the RADIUS server and device and avoid RADIUS packets from being tampered with, configure the same shared key on the RADIUS server and device.
- To use the RADIUS server for authentication and authorization, perform the following tasks on the device:
  - **c.** Create a RADIUS scheme.
  - **d.** Specify the RADIUS server as the authentication and authorization server in the RADIUS scheme.
  - **e.** Apply the RADIUS scheme to the ISP domain of the 802.1X user.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software versions
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later
S6525XE-HI switch series	Release 6008 and later
S5850 switch series	Release 8005 and later
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release

Hardware	Software versions
	6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx

Hardware	Software versions
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

As a best practice to avoid valid users from being blocked, do not enable 802.1X globally before you finish all settings.

802.1X settings take effect on an interface only when 802.1X is enabled both globally and on the interface.

Procedures

Configuring the RADIUS server (Device B)

In this example, an H3C switch acts as the RADIUS server.

Create a network access user named **dot1x** and enter its view.

```
<DeviceB> system-view
[DeviceB] local-user dot1x class network
New local user added.
```

Set the password to **123456TESTplat&!** in plaintext form for user **dot1x**.

```
[DeviceB-luser-network-dot1x] password simple 123456TESTplat&!
```

Specify VLAN 4 as the authorization VLAN.

```
[DeviceB-luser-network-dot1x] authorization-attribute vlan 4
[DeviceB-luser-network-dot1x] quit
```

Specify the RADIUS client at 10.1.1.2 and set the shared key to **expert** in plaintext form.

```
[DeviceB] radius-server client ip 10.1.1.2 key simple expert
```

Activate RADIUS client and user settings.

```
[DeviceB] radius-server activate
```

Configuring the NAS (Device A)

1. Configure a RADIUS scheme:

Create a RADIUS scheme named **rad** and enter its view.

```
<DeviceA> system-view
[DeviceA] radius scheme rad
New RADIUS scheme.
```

Specify the server at 10.1.1.1 as the primary authentication server, and set the shared key to **expert** in plain text for secure communication between the authentication server and the device.

```
[DeviceA-radius-rad] primary authentication 10.1.1.1 key simple expert
```

Exclude the ISP domain name from the usernames sent to the RADIUS server.

```
[DeviceA-radius-rad] user-name-format without-domain
[DeviceA-radius-rad] quit
```

2. Configure an ISP domain:

Create an ISP domain named **bbb** and enter its view.

```
[DeviceA] domain bbb
```

Configure the ISP domain to use RADIUS scheme **rad** for LAN user authentication and authorization, and do not perform accounting for LAN users in the domain.

```
[DeviceA-isp-bbb] authentication lan-access radius-scheme rad
[DeviceA-isp-bbb] authorization lan-access radius-scheme rad
[DeviceA-isp-bbb] accounting lan-access none
[DeviceA-isp-bbb] quit
```

3. Configure 802.1X authentication:

Enable 802.1X on interface GigabitEthernet 1/0/1.

```
[DeviceA] interface gigabitethernet1/0/1
[DeviceA-GigabitEthernet1/0/1] dot1x
```

Specify ISP domain **bbb** as the mandatory authentication domain on interface GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[DeviceA-GigabitEthernet1/0/1] quit
```

Enable 802.1X globally.

```
[DeviceA] dot1x
```

Configuring the 802.1X client

Restrictions and guidelines

This example uses iNode PC 7.3 (E0518) to describe the procedure.

If the host runs the Windows XP built-in 802.1X client, configure the network connection properties as follows:

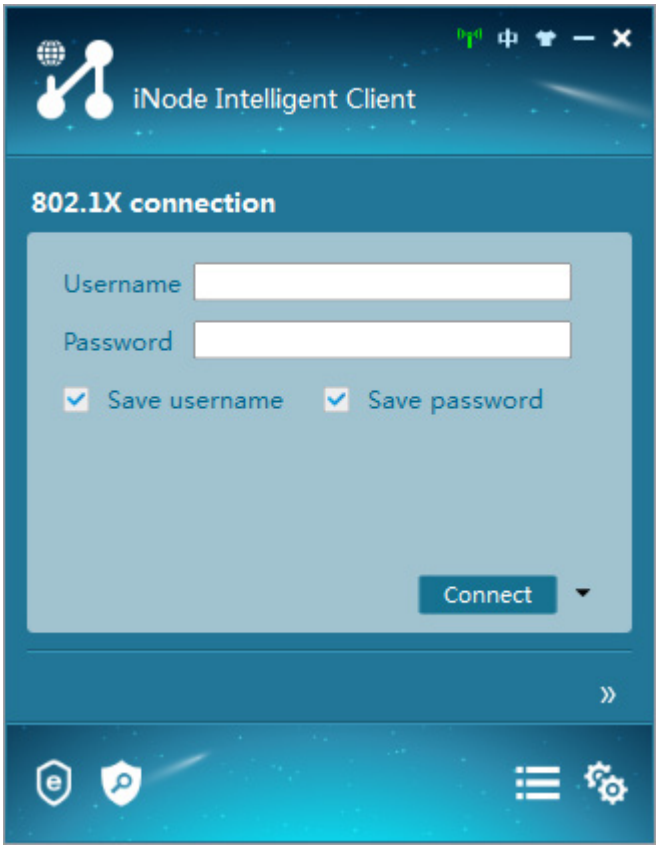
1. Click the **Authentication** tab of the properties window.
2. Select the **Enable IEEE 802.1X authentication for this network** option.
3. Select MD5 challenge as the EAP type.
4. Click **OK**.

Make sure the client can update its IP address to access the resources in the authorized VLAN after passing authentication.

Procedure

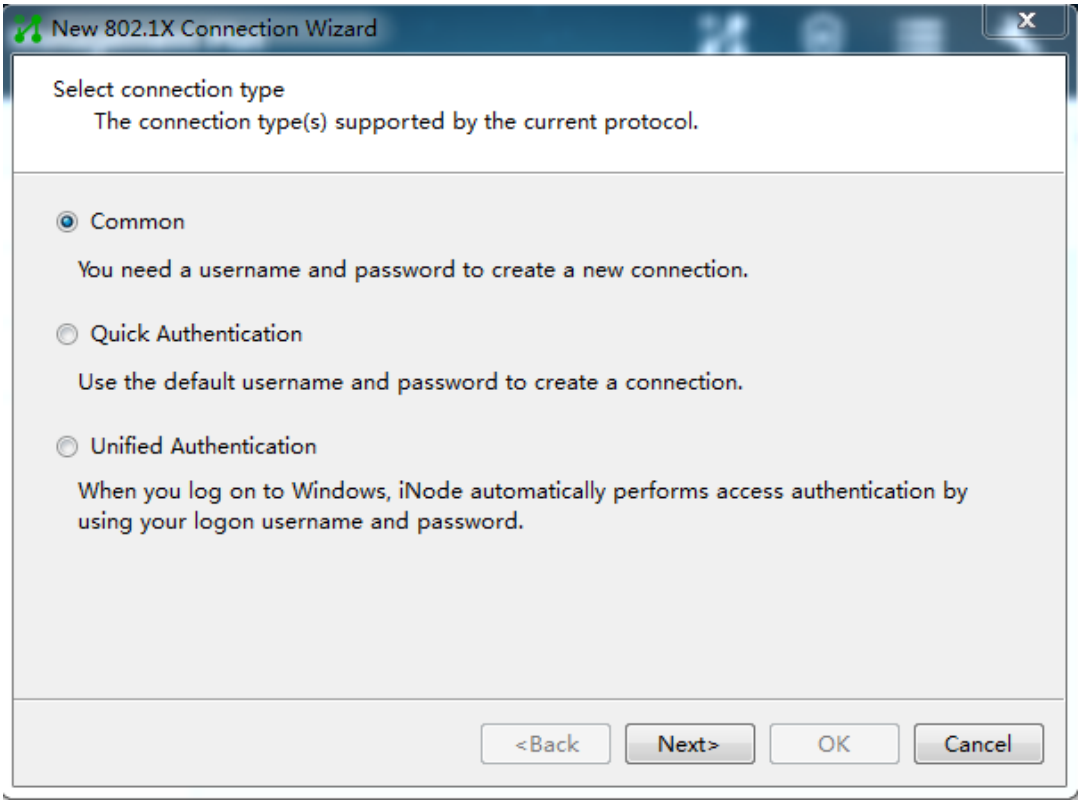
1. Run the iNode client.

   Figure 8 iNode client



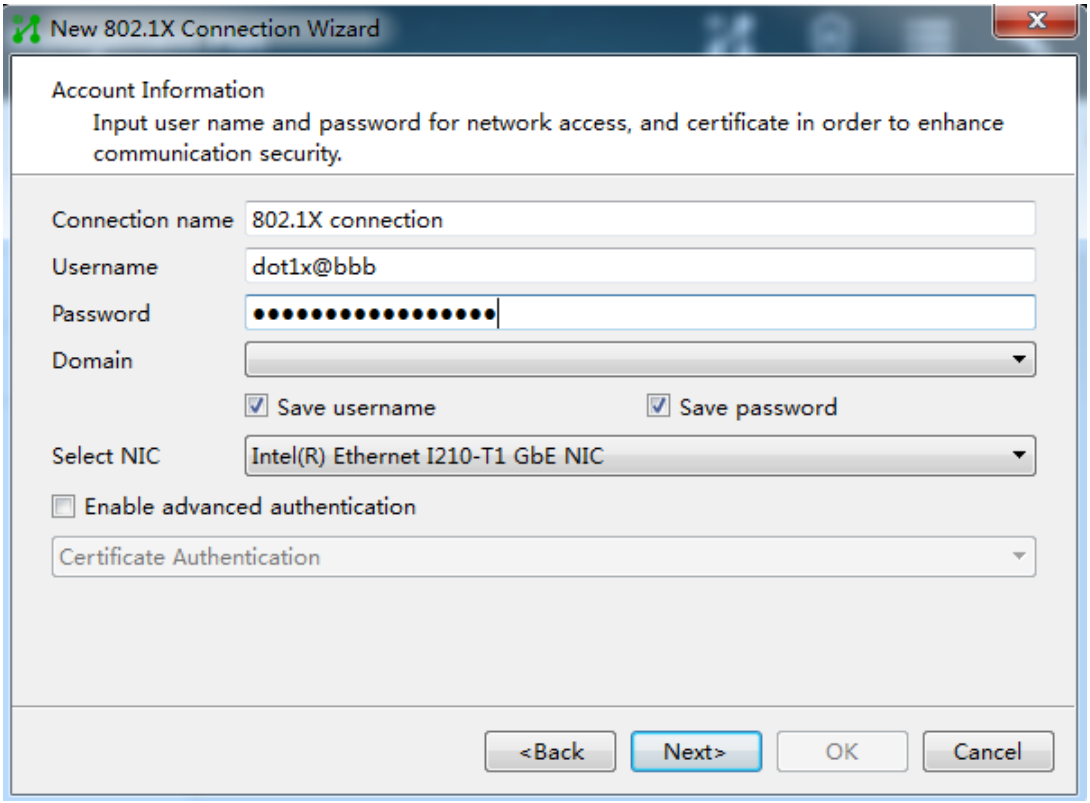
2. Create a new 802.1X connection.
3. On the **New 802.1X Connection Wizard** window, select **Common**, and then click **Next**.

Figure 9 Creating a new 802.1X connection



4. Configure the connection name, username, and password, and then click **Next**.

Figure 10 Configuring the connection name, username, and password



For authentication to be performed correctly, the following details must comply with the correlation rules shown in Table 1:

- Username specified on the iNode client.
- Domain and username format configuration on the access device.
- Service suffix on IMC.

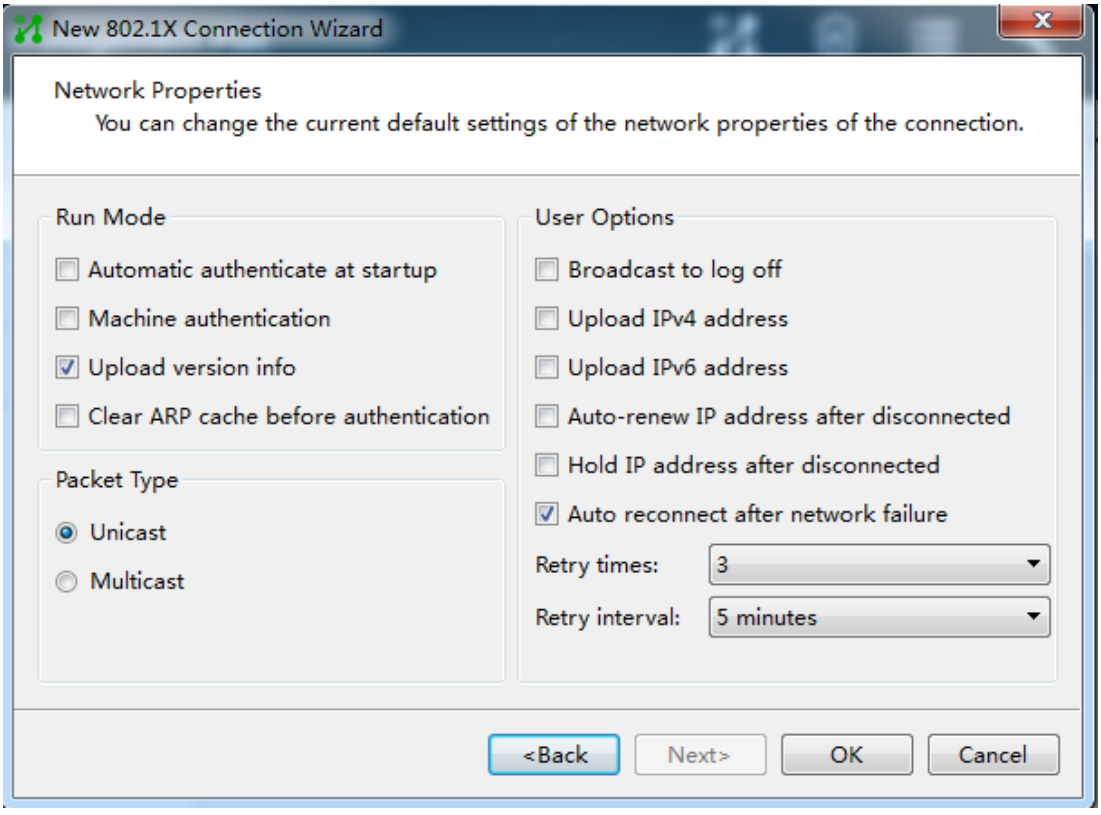
Table 1 Parameter correlation

Username format on the iNode client	Domain on the access device	Username format configured on the access device	Service suffix on IMC
X@Y	Y	with-domain	Y
X@Y	Y	without-domain	No suffix
X	Default domain (the default domain specified on the access device)	with-domain	Name of the default domain
X	Default domain (the default domain specified on the access device)	without-domain	No suffix

5. Configure the network property settings, and then click **OK**.

   If you set local authentication as the backup authentication method, do not select **Upload version info** in the **Run Mode** area. The access device cannot recognize the version number in EAP packets.

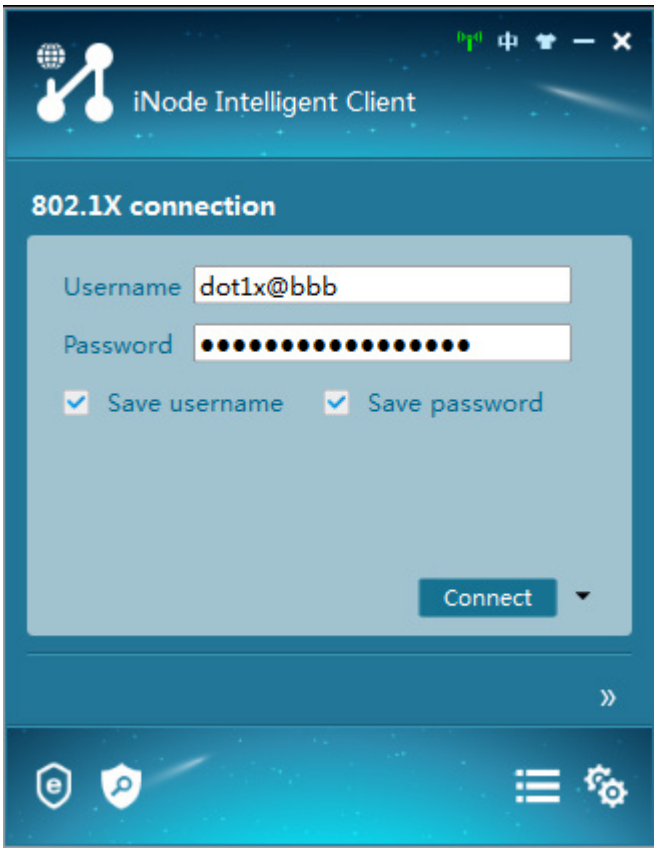
Figure 11 Configuring 802.1X connection properties



6. Initiate the 802.1X connection.

Enter the username and password on the iNode client, and then click **Connect**.

Figure 12 Initiating the 802.1X connection



Verifying the configuration

IMPORTANT:

Support for VSI-related fields depends on the device model.

On Device B, display all active RADIUS clients and RADIUS users.

```
[DeviceB] display radius-server active-client
Total 1 RADIUS clients.
Client IP: 10.1.1.2
[DeviceB] display radius-server active-user dot1x
Total 1 RADIUS users matched.
Username: dot1x
  Description: Not configured
  Authorization attributes:
    VLAN ID: 4
    ACL number: Not configured
  Validity period:
    Expiration time: Not configured
```

On Device A, display online 802.1X user information.

```
[DeviceA] display dot1x connection
Total connections: 1
```

```
Slot ID: 1
User MAC address: 0010-9400-0021
Access interface: GigabitEthernet1/0/1
Username: dot1x@bbb
User access state: Successful
Authentication domain: bbb
EAP packet identifier: 4
Authentication method: CHAP
Initial VLAN: 2
Authorization untagged VLAN: N/A
Authorization tagged VLAN list: N/A
Authorization VSI: N/A
Authorization microsegment ID: N/A
Authorization ACL number/name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Start accounting: Successful
Real-time accounting-update failures: 0
Termination action: Default
Session timeout period: 86400 s
Online from: 2013/01/20 07:58:10
Online duration: 0h 0m 40s
```

Configuration files

- Device A:

```
#
 dot1x
#
radius scheme rad
 primary authentication 10.1.1.1 key cipher
$c$3$l+xIXR7hboPo33+MkEf/01WsnVHhxZCeYg==
 user-name-format without-domain
#
 domain bbb
 authentication lan-access radius-scheme rad
 authorization lan-access radius-scheme rad
 accounting lan-access none
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
 dot1x mandatory-domain bbb
#
```

- Device B:

```
#
local-user dot1x class network
```

```
 password cipher $c$3$GuUyAQq0JHH6iBF38xsnB/tQEPTZhTAMIGLweOXr2uPbqJ0=
 authorization-attribute vlan 4
 authorization-attribute user-role network-operator
#
 radius-server client ip 10.1.1.2 key cipher
$c$3$Po5RD6PcGZi+V6l6Nx7hpiLZNSMeOjbUzQ==
#
 radius-server activate
#
```

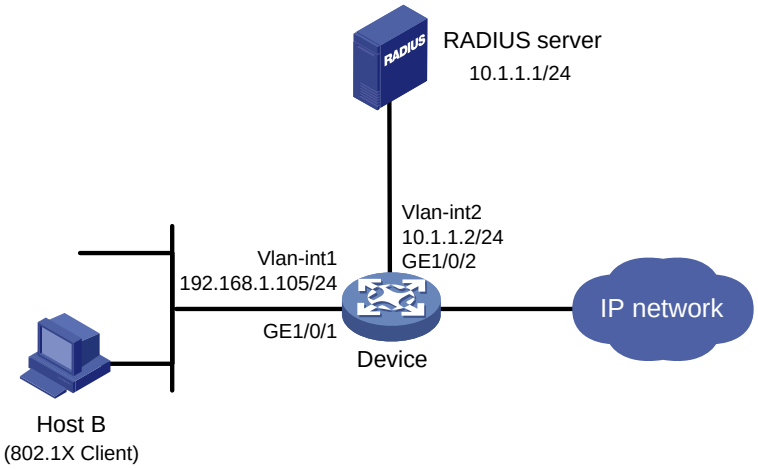
Example: Configuring 802.1X unicast trigger

Network configuration

As shown in Figure 13:

- The device uses the RADIUS server for 802.1X user authentication and authorization.
- IMC acts as the RADIUS server.
- The user on Host B uses the Windows XP built-in 802.1X client to interact with the device for 802.1X authentication.

Figure 13 Network diagram



Analysis

- For the device to use the RADIUS server for user authentication, perform the following tasks on the RADIUS server:
  - **a.** Add the device as an access device to the RADIUS server.
  - **b.** Add an access policy.
  - **c.** Add an access service and specify the access policy in the access service.
  - **d.** Add an access user and specify the access service for the access user.

- For the device to perform RADIUS-based authentication and authorization for the 802.1X user, configure AAA settings on the device, including ISP domain settings and RADIUS scheme settings.
- Because the Windows XP built-in 802.1X client cannot initiate 802.1X connection, you must enable an authentication trigger feature on the device. As a best practice to ensure system performance, disable 802.1X multicast trigger and enable unicast trigger. In multicast trigger mode, the device multicasts a large number of Identity EAP-Request packets periodically to the host, which consumes bandwidth and system resources.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software versions
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch	Release 63xx

Hardware	Software versions
S5500V3-48P-SI switch	
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

Hardware	Software versions
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

As a best practice to avoid duplicate authentication packets, disable multicast trigger on an interface if unicast trigger is enabled on that interface.

Prerequisites

Configure IP addresses for interfaces, as shown in Figure 13. Make sure the host, device, and server are reachable.

Procedures

Configuring the RADIUS server

This example uses IMC PLAT 7.3 (E0506), IMC EIA 7.3 (E0503), and IMC EIP 7.3 (E0503) to describe the procedure.

Adding the device to the IMC Platform as an access device

1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.
4. Click **Add**.
5. On the page that opens, configure access device parameters.
   a. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   b. Set the shared key to **expert** for secure authentication and accounting communication, and confirm the shared key.
   c. Select **H3C (General)** from the **Access Device Type** list.
   d. Select an access device from the device list or manually add an access device. In this example, the device IP address is 10.1.1.2.
   e. Use the default values for other parameters.
   f. Click **OK**.

   The IP address of the access device specified on the RADIUS server must be the same as the source IP address of the RADIUS packets sent from the device. On the device, the source IP address is chosen in the following order:

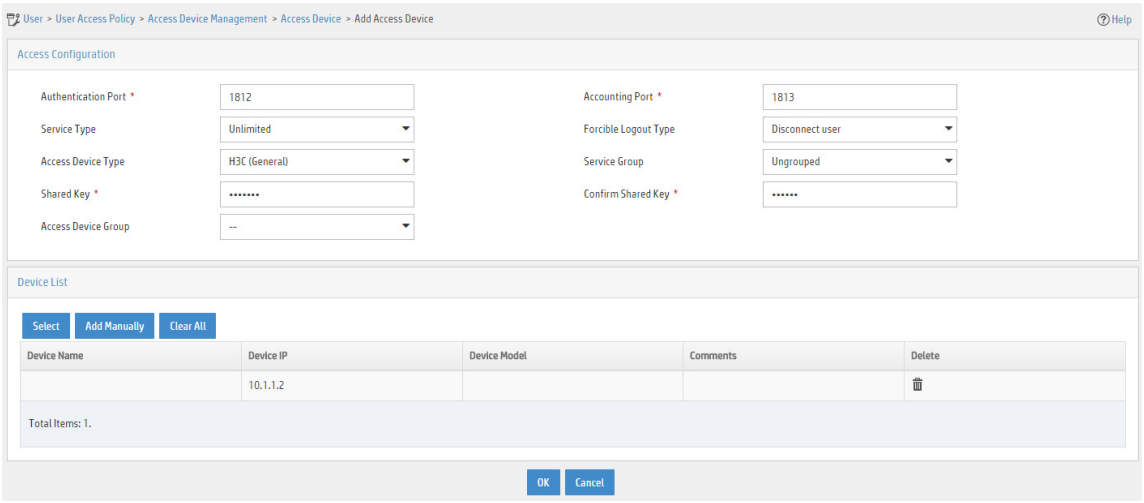
   a. IP address specified by using the **`nas-ip`** command.

b. IP address specified by using the **`radius nas-ip`** command.

c. IP address of the outbound interface (the default).

In this example, the device uses the IP address of the outbound interface as the source IP address of RADIUS packets.

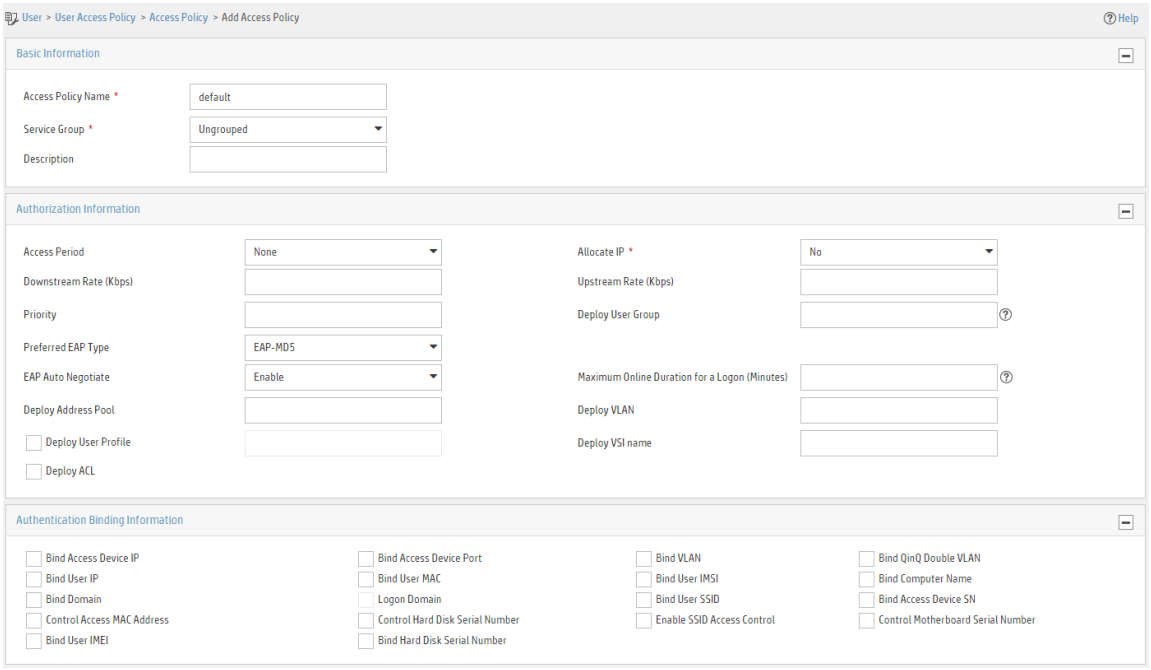
Figure 14 Adding an access device



Adding an access policy

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Policy**.
3. Click **Add**.
4. On the page that opens, configure access policy parameters.
   a. Enter access policy name **default**.
   b. Use the default values for other parameters.
   c. Click **OK**.

Figure 15 Adding an access policy



Adding an access service

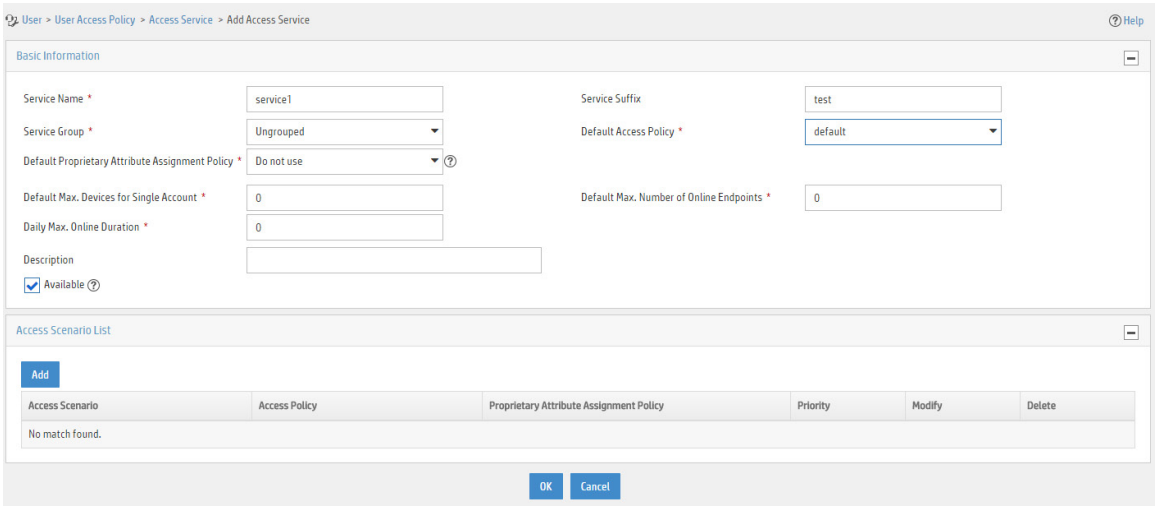
1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Service**.
3. Click **Add**.
4. On the page that opens, configure access service parameters.
   a. Enter service name **service1** and set the service suffix to **test**. The service suffix is the authentication domain for the 802.1X user.

   IMPORTANT:

   With the service suffix configured, you must configure the device to send usernames that include the domain name to the RADIUS server. By default, the device includes the domain name in the usernames sent to a RADIUS server.

   b. Select **default** from the **Default Access Policy** list.
   c. Use the default values for other parameters.
   d. Click **OK**.

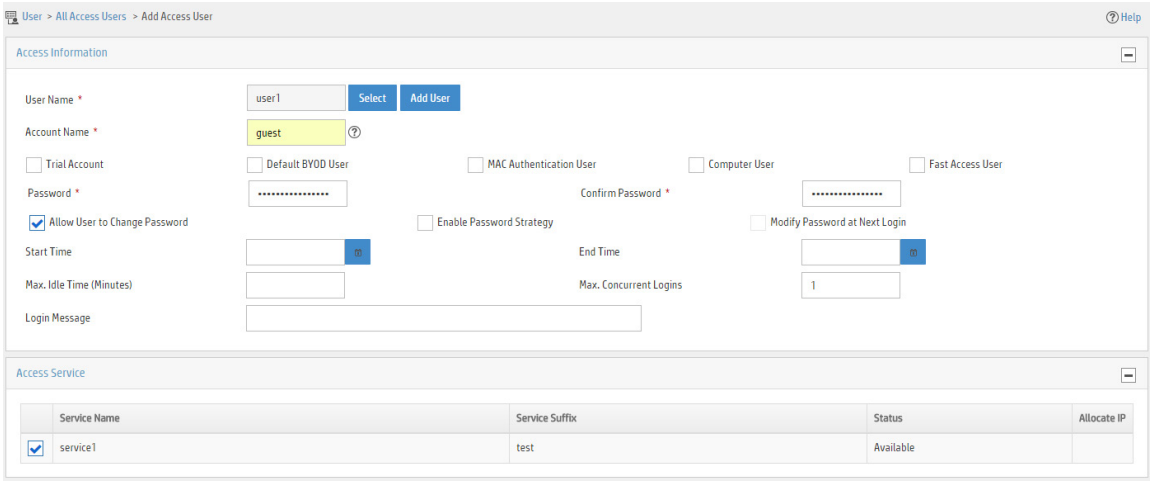
Figure 16 Adding an access service



Adding an access user

1. Click the **User** tab.
2. From the navigation pane, select **Access User** > **Access User**.
3. Click **Add**.
4. On the page that opens, configure access user parameters.
   a. Click **Add User** to add a user named **user1**.
   b. Enter account name **guest** and password **123456TESTplat&!**. The device uses the account name to identify the user when the user accesses the network.
   c. Select **service1** in the **Access Service** area.
   d. Use the default values for other parameters.
   e. Click **OK**.

Figure 17 Adding an access user



Configuring the device

Create VLANs and VLAN interfaces, and assign IP addresses to interfaces. (Details not shown.)

Create a RADIUS scheme named **radius1** and enter its view.

```
<Device> system-view
[Device] radius scheme radius1
```

Specify the RADIUS server at 10.1.1.1 as the primary authentication server.

```
[Device-radius-radius1] primary authentication 10.1.1.1
```

Set the shared key to **expert** in plaintext form for secure communication with the RADIUS authentication server.

```
[Device-radius-radius1] key authentication simple expert
```

Create an ISP domain named **test** and enter its view.

```
[Device] domain test
```

Configure the ISP domain to use RADIUS scheme **radius1** for LAN user authentication and authorization in the domain.

```
[Device-isp-test] authentication lan-access radius-scheme radius1
[Device-isp-test] authorization lan-access radius-scheme radius1
[Device-isp-test] quit
```

Configure domain **test** as the default domain.

```
[Device] domain default enable test
```

Disable 802.1X multicast trigger on interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] undo dot1x multicast-trigger
```

Enable 802.1X unicast trigger on interface GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet 1/0/1] dot1x unicast-trigger
```

Enable 802.1X on interface GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
```

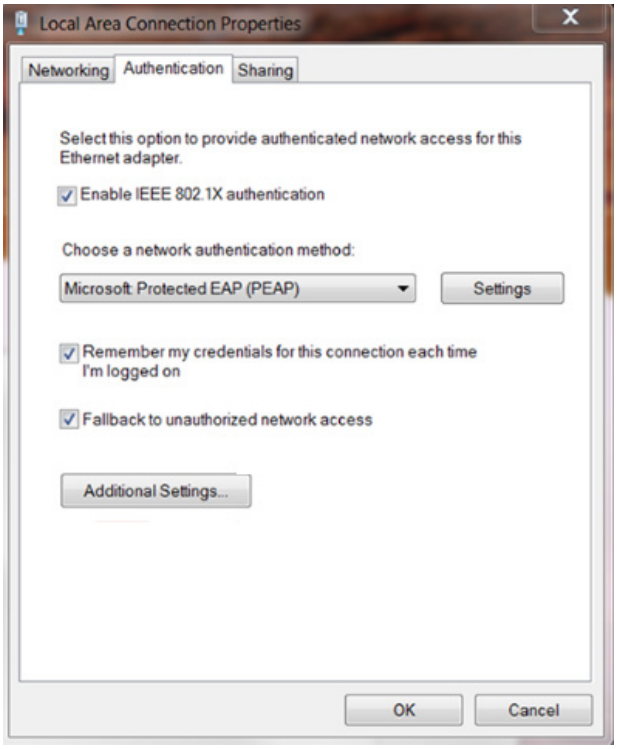
Enable 802.1X globally.

```
[Device] dot1x
```

Configuring the 802.1X client

This example uses the Windows XP built-in 802.1X client to describe the procedure. The configuration is as shown in Figure 18.

Figure 18 Configuring the Windows XP built-in 802.1X client



Verifying the configuration

Verify that you can use the user account to pass 802.1X authentication:

Use the host to visit an Internet webpage. The Windows status bar displays a message and asks you to enter your username and password.

Enter username **guest@test** and password **123456TESTplat&!**.

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
 domain default enable test
#
 dot1x
#
radius scheme radius1
 primary authentication 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain test
 authentication default radius-scheme radius1
 authorization default radius-scheme radius1
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 undo dot1x multicast-trigger
 dot1x
 dot1x unicast-trigger
#
```

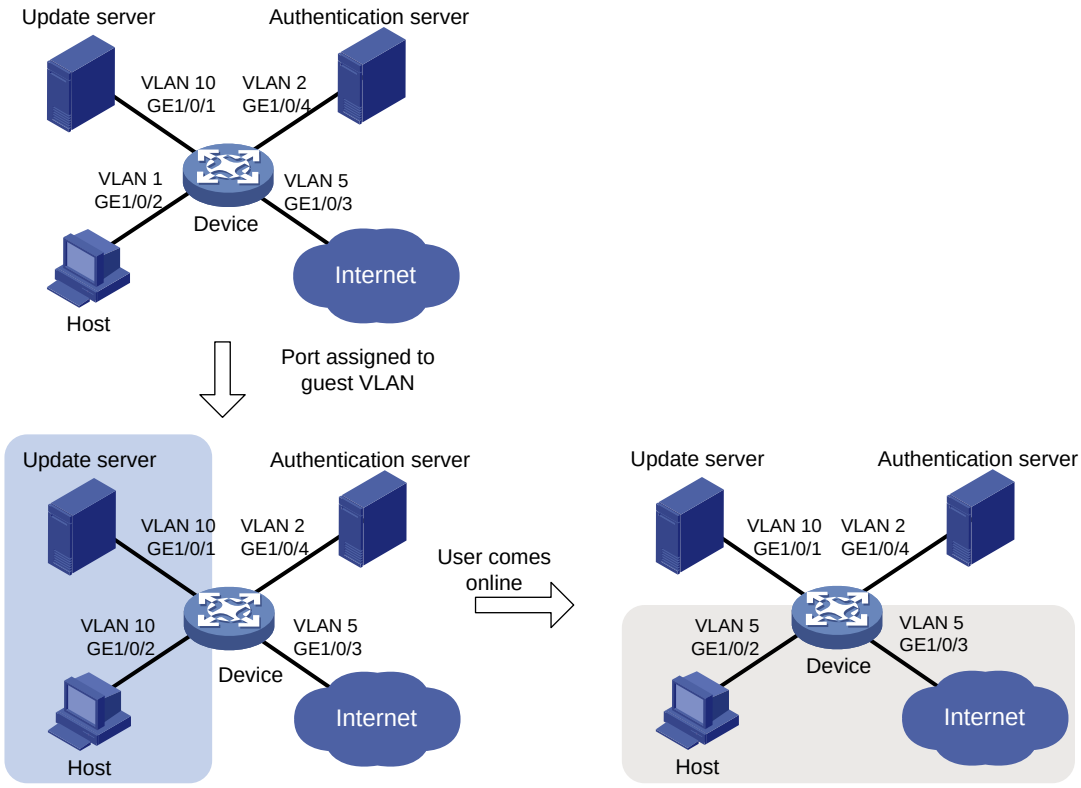
Example: Configuring 802.1X with guest VLAN and authorization VLAN assignment

Network configuration

As shown in Figure 19:

- Use a RADIUS server to perform authentication, authorization, and accounting for 802.1X users that connect to GigabitEthernet 1/0/2. Implement port-based access control on the port.
- Configure VLAN 10 as the 802.1X guest VLAN on GigabitEthernet 1/0/2. The host and the update server are both in VLAN 10, and the host can access the update server and download the 802.1X client software.
- To prevent users in the guest VLAN from accessing the Internet, apply a QoS policy to the outbound direction of VLAN 10 to filter packets destined for the Internet (5.1.1.1).
- After the host passes 802.1X authentication, the access device assigns the host to the same VLAN (VLAN 5) as the interface (GigabitEthernet 1/0/3) for Internet access.

Figure 19 Network diagram



Analysis

- For the 802.1X user on the host to access the update server before it passes authentication, configure VLAN 10 as the guest VLAN on the port connected to the host.
- For the 802.1X user on the host to access the Internet after it passes authentication, specify VLAN 5 (the VLAN connected to the Internet) as the user's authorization VLAN. After the user passes 802.1X authentication, the port connected to the host is assigned to VLAN 5.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software versions
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch	Release 63xx

Hardware	Software versions
S5500V3-48P-SI switch	
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx

Hardware	Software versions
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

- On a port that performs MAC-based access control, the 802.1X guest VLAN feature has higher priority than the block MAC action and has lower priority than the shutdown port action of the port intrusion protection feature. For more information about the actions of the port intrusion protection feature, see port security configuration in *Security Configuration Guide*.
- Assign different IDs to the port VLAN, the voice VLAN, and the 802.1X guest VLAN on a port. The assignment makes sure the port can correctly process incoming VLAN-tagged traffic. For more information about VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- You cannot specify a VLAN as both a super VLAN and an 802.1X guest VLAN.

Procedures

For information about the ISP domain and RADIUS commands used on the device in this example, see AAA commands in *Security Command Reference*.

Configuring the RADIUS server

This example uses IMC PLAT 7.3 (E0506), IMC EIA 7.3 (E0503), and IMC EIP 7.3 (E0503) to describe the procedure.

Adding the device to the IMC Platform as an access device

1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.
4. Click **Add**.
5. On the page that opens, configure access device parameters.
   a. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   b. Select **H3C (General)** from the **Access Device Type** list.
   c. Set the shared key to **expert** for secure authentication and accounting communication.
   d. Select an access device from the device list or manually add an access device. In this example, the IP address of the access device is 10.1.1.2.
   e. Use the default values for other parameters.
   f. Click **OK**.

The IP address of the access device specified on the RADIUS server must be the same as the source IP address of the RADIUS packets sent from the device. On the device, the source IP address is chosen in the following order:

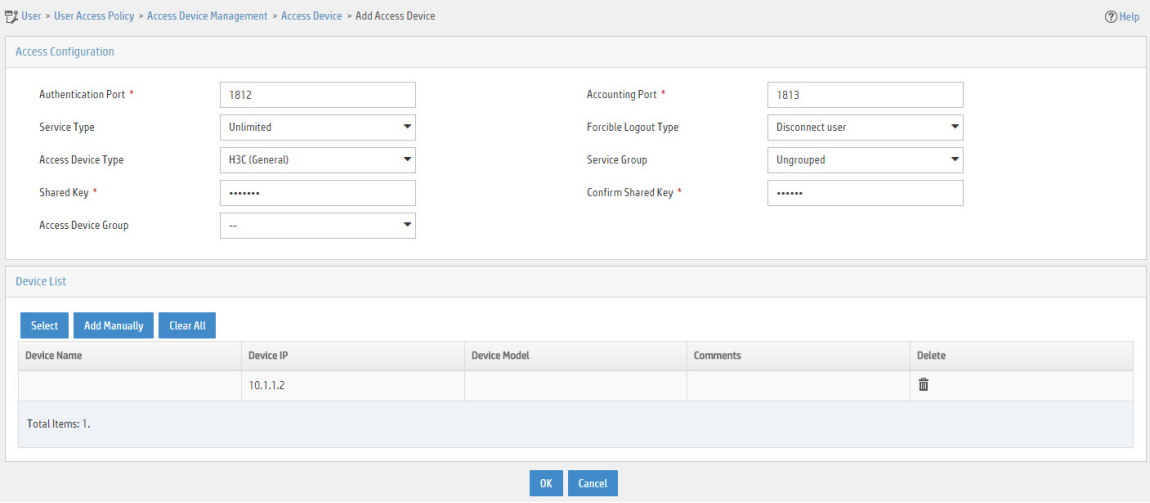
a. IP address specified by using the **`nas-ip`** command.

b. IP address specified by using the **`radius nas-ip`** command.

c. IP address of the outbound interface (the default).

In this example, the device uses the IP address of the outbound interface as the source IP address of RADIUS packets.

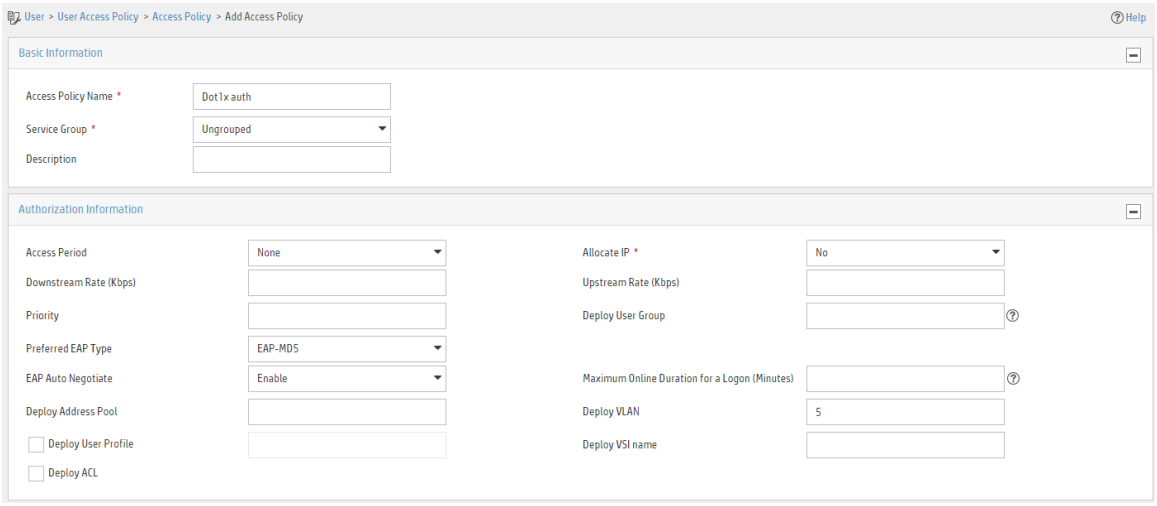
Figure 20 Adding an access device



Adding an access policy

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Policy**.
3. Click **Add**.
4. On the page that opens, configure access policy parameters.
   a. Enter access policy name **Dot1x auth**.
   b. Enter **5** in the **Deploy VLAN** field.
   c. Configure other parameters as needed.
   d. Click **OK**.

Figure 21 Adding an access policy



Adding an access service

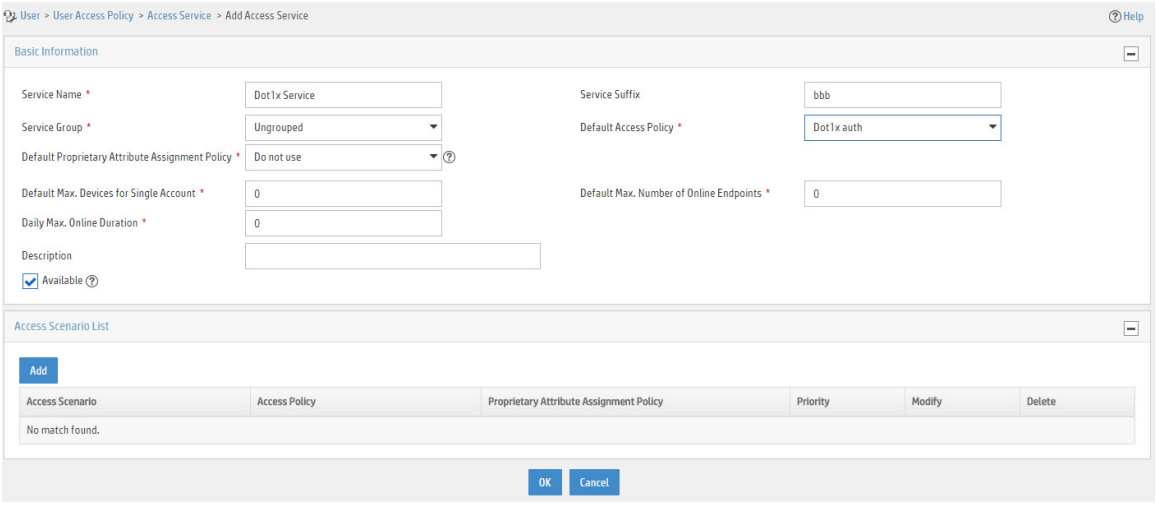
1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Service**.
3. Click **Add**.
4. On the page that opens, configure access service parameters.
   a. Enter service name **Dot1x Service** and set the service suffix to **bbb**. The service suffix is the authentication domain for the 802.1X user.

   IMPORTANT:

   With the service suffix configured, you must configure the device to send usernames that include the domain name to the RADIUS server.

   b. Select **Dot1x auth** from the **Default Access Policy** list.
   c. Configure other parameters as needed.
   d. Click **OK**.

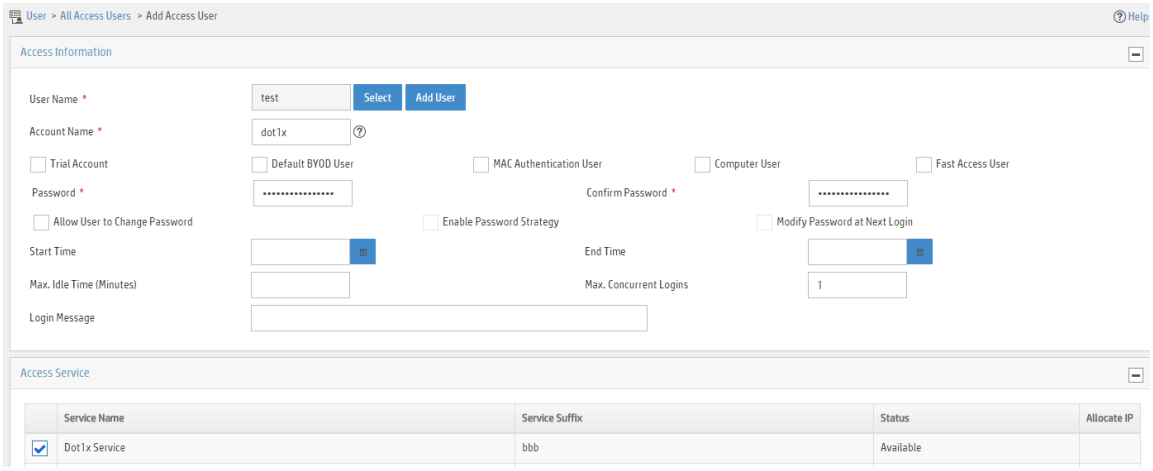
Figure 22 Adding an access service



Adding an access user

1. Click the **User** tab.
2. From the navigation pane, select **Access User** > **Access User**.
3. Click **Add**.
4. On the page that opens, configure access user parameters.
   a. Select the user or add a user named **test**.
   b. Enter account name **dot1x** and password **123456TESTplat&!**.
   c. Select **Dot1x Service** in the **Access Service** area.
   d. Configure other parameters as needed.
   e. Click **OK**.

Figure 23 Adding an access user



Configuring the device

1. Create VLANs, and assign ports to the VLANs.

   NOTE:

   By default, VLAN 1 exists and all ports belong to the VLAN. You do not need to create the VLAN or assign GigabitEthernet 1/0/2 to the VLAN.

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 1/0/3
[Device-vlan5] quit
```

2. Configure a QoS policy to filter VLAN 10 traffic destined for the Internet (5.1.1.1):

   # Configure advanced ACL 3000 to match the packets destined for 5.1.1.1.

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip destination 5.1.1.1 0.0.0.255
```

```
[Device-acl-ipv4-adv-3000] quit
```

Create a traffic class named **classifier_1** and use ACL 3000 as the match criterion.

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 3000
[Device-classifier-classifier_1] quit
```

Create a traffic behavior named **behavior_1** and add a deny filter action to drop packets.

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] filter deny
[Device-behavior-behavior_1] quit
```

Create a QoS policy named **policy_1**. Associate traffic class **classifier_1** with traffic behavior **behavior_1** in the QoS policy.

```
[Device] qos policy policy_1
[Device-qospolicy-policy_1] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy_1] quit
```

Apply QoS policy **policy_1** to the outbound direction of VLAN 10.

```
[Device] qos vlan-policy policy_1 vlan 10 outbound
```

3. Configure a RADIUS scheme:

Create a RADIUS scheme named **2000** and enter RADIUS scheme view.

```
[Device] radius scheme 2000
```

Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```

Specify the server at 10.1.1.1 as the primary accounting server, and set the accounting port to 1813.

```
[Device-radius-2000] primary accounting 10.1.1.1 1813
```

Set the shared key to **expert** in plaintext form for secure communication between the authentication server and the device.

```
[Device-radius-2000] key authentication simple expert
```

Set the shared key to **expert** in plaintext form for secure communication between the accounting server and the device.

```
[Device-radius-2000] key accounting simple expert
```

Include the ISP domain name in the usernames sent to the RADIUS server. This step is optional. By default, the ISP domain name is included in the usernames sent to a RADIUS server.

```
[Device-radius-2000] user-name-format with-domain
[Device-radius-2000] quit
```

4. Configure an ISP domain:

Create ISP domain **bbb** and enter ISP domain view.

```
[Device] domain bbb
```

Apply RADIUS scheme **2000** to the ISP domain for LAN user authentication, authorization, and accounting.

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

5. Configure 802.1X:

Enable 802.1X on interface GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] dot1x
```

Enable 802.1X port-based access control on the interface.

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

Set the port authorization mode to **auto**. This step is optional. By default, the port uses the auto mode.

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
```

Specify VLAN 10 as the 802.1X guest VLAN on interface GigabitEthernet 1/0/2.

```
[Device-GigabitEthernet1/0/2] dot1x guest-vlan 10
[Device-GigabitEthernet1/0/2] quit
```

Enable 802.1X globally.

```
[Device] dot1x
```

Configuring the 802.1X client

Configure the 802.1X client. Make sure the 802.1X client can update its IP address after the access port is assigned to the guest VLAN or an authorization VLAN. (Details not shown.)

Verifying the configuration

Verify the 802.1X guest VLAN configuration on GigabitEthernet 1/0/2.

```
[Device] display dot1x interface gigabitethernet 1/0/2
```

Verify that GigabitEthernet 1/0/2 is assigned to VLAN 10 before any user passes authentication on the port.

```
[Device] display vlan 10
```

After a user passes authentication, display information on GigabitEthernet 1/0/2. Verify that GigabitEthernet 1/0/2 is assigned to VLAN 5.

```
[Device] display interface gigabitethernet 1/0/2
```

Configuration files

```
#
 vlan 2
#
 vlan 5
#
 vlan 10
#
acl advanced 3000
 rule 0 permit ip destination 5.1.1.0 0.0.0.255
#
traffic classifier classifier_1 operator and
 if-match acl 3000
#
traffic behavior behavior_1
 filter deny
#
qos policy policy_1
```

```
 classifier classifier_1 behavior behavior_1
#
 qos vlan-policy policy_1 vlan 10 outbound
#
radius scheme 2000
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
 key accounting cipher $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain bbb
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 accounting lan-access radius-scheme 2000
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 dot1x
 dot1x port-method portbased
 dot1x guest-vlan 10
#
interface GigabitEthernet1/0/3
 port access vlan 5
#
interface GigabitEthernet1/0/4
 port access vlan 2
#
 dot1x
#
```

Example: Configuring 802.1X with ACL assignment

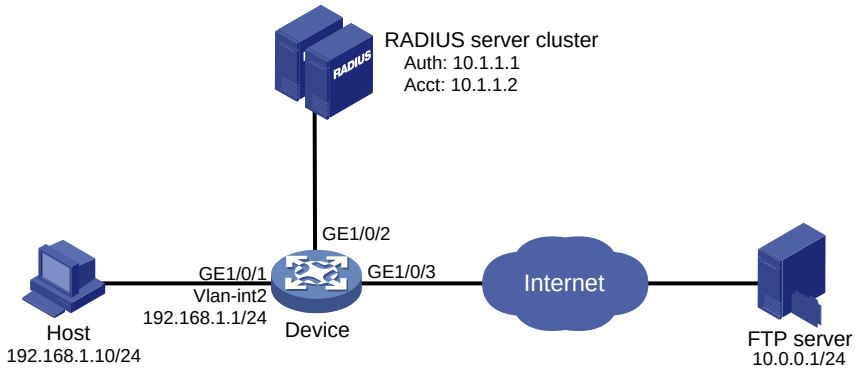
Network configuration

As shown in Figure 24, the user on the host that connects to GigabitEthernet 1/0/1 must pass 802.1X authentication to access the Internet.

Perform 802.1X authentication on GigabitEthernet 1/0/1. Use the RADIUS server at 10.1.1.1 as the authentication and authorization server, and the RADIUS server at 10.1.1.2 as the accounting server.

Configure ACL assignment on GigabitEthernet 1/0/1 to deny access of 802.1X users to the FTP server from 8:00 to 18:00 on weekdays.

Figure 24 Network diagram



Analysis

- For the device to use the RADIUS server for user authentication, perform the following tasks on the RADIUS server:
  a. Add the device as an access device to the RADIUS server.
  b. Add an access policy.
  c. Add an access service and specify the access policy in the access service.
  d. Add an access user and specify the access service for the access user.
- For the device to perform RADIUS-based authentication and authorization for the 802.1X user, configure AAA settings on the device, including ISP domain settings and RADIUS scheme settings.
- To assign an ACL to the user after the user passes authentication and use the ACL to restrict the user's access behaviors, perform the following tasks:
  - Specify the ACL in the user account on the RADIUS server.
  - Create the ACL and configure its rules on the device.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software versions
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release

Hardware	Software versions
	6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series	Release 63xx

Hardware	Software versions
S3100V3-SI switch series	
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

- If the server assigns both an authorization ACL and microsegment to an 802.1X authentication user on a microsegmented network, only the authorization microsegment takes effect.
- In this example, the RADIUS server assigns only an ACL number to the 802.1X user. You must manually create the ACL and configure its rules on the device.
- To change the access permissions of the 802.1X user, you can use one of the following methods:
  - Modify ACL rules in the authorization ACL on the device.
  - Assign another ACL to the user as the authorization ACL from the RADIUS server.

Procedures

For information about the ISP domain and RADIUS commands used on the device in this example, see AAA commands in *Security Command Reference*.

Configuring the RADIUS server

This example uses IMC PLAT 7.3 (E0506), IMC EIA 7.3 (E0503), and IMC EIP 7.3 (E0503) to describe the procedure.

Adding the device to the IMC Platform as an access device

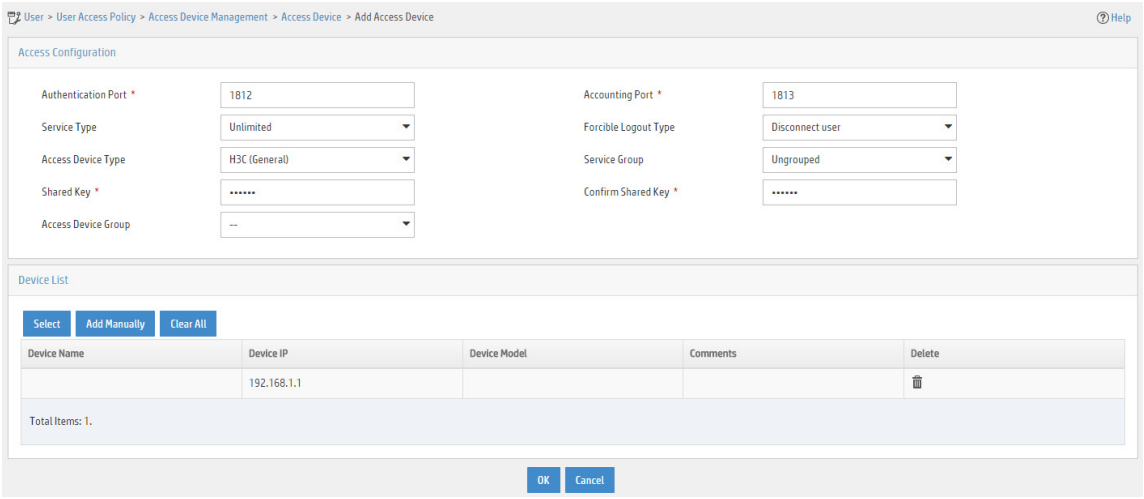
1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.
4. Click **Add**.
5. On the page that opens, configure access device parameters.
   a. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   b. Select **H3C (General)** from the **Access Device Type** list.
   c. Set the shared key to **expert** for secure authentication and accounting communication.
   d. Select an access device from the device list or manually add an access device. In this example, the device IP address is 192.168.1.1.
   e. Use the default values for other parameters and click **OK**.

   The IP address of the access device specified on the RADIUS server must be the same as the source IP address of the RADIUS packets sent from the device. On the device, the source IP address is chosen in the following order:

   a. IP address specified by using the **`nas-ip`** command.
   b. IP address specified by using the **`radius nas-ip`** command.
   c. IP address of the outbound interface (the default).

   In this example, the device uses the IP address of the outbound interface as the source IP address of RADIUS packets.

Figure 25 Adding an access device



Adding an access policy

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Policy**.
3. Click **Add**.
4. On the page that opens, configure access policy parameters.

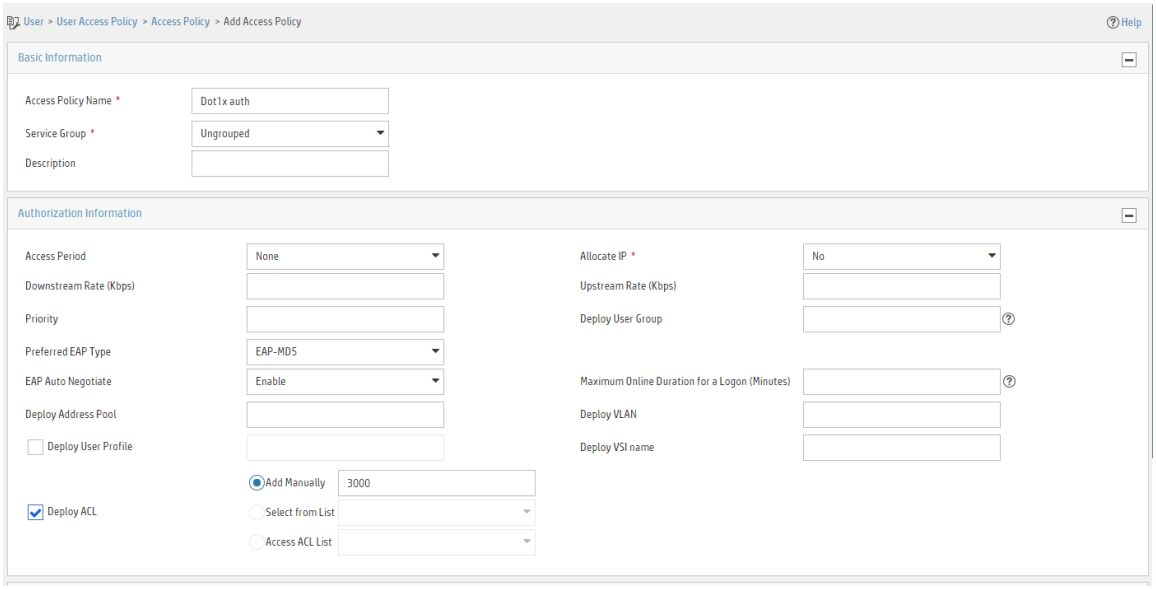
a. Enter access policy name **Dot1x auth**.

b. In the **Authorization Information** area, select **Deploy ACL** and manually enter ACL number **3000**.

c. Configure other parameters as needed.

d. Click **OK**.

Figure 26 Adding an access policy



Adding an access service

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Service**.
3. Click **Add**.
4. On the page that opens, configure access service parameters.

   a. Enter service name **Dot1x Service** and set the service suffix to **bbb**. The service suffix is the authentication domain for the 802.1X user.

   IMPORTANT:

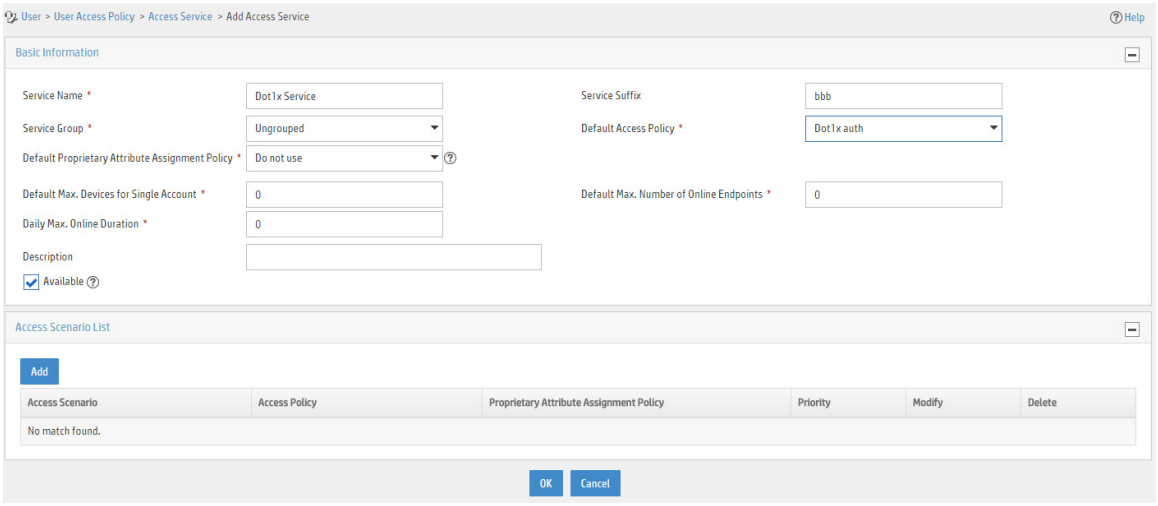
   With the service suffix configured, you must configure the device to send usernames that include the domain name to the RADIUS server.

   b. Select **Dot1x auth** from the **Default Access Policy** list.

   c. Configure other parameters as needed.

   d. Click **OK**.

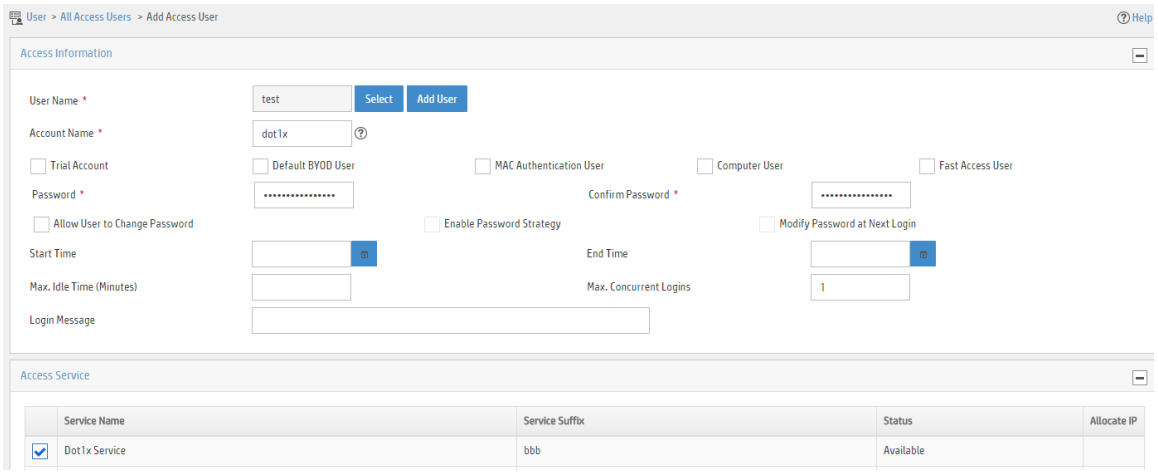
Figure 27 Adding an access service



Adding an access user

1. Click the **User** tab.
2. From the navigation pane, select **Access User** > **Access User**.
3. Click **Add**.
4. On the page that opens, configure user parameters.
   a. Select the user or add a user named **test**.
   b. Enter account name **dot1x** and password **123456TESTplat&!**.
   c. Select **Dot1x Service** in the **Access Service** area.
   d. Configure other parameters as needed.
   e. Click **OK**.

Figure 28 Adding an access user



Configuring the device

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure a RADIUS scheme.

IMPORTANT:

With the service suffix configured on IMC, you must configure the device to send usernames that include the domain name to the RADIUS server. By default, the device includes the domain name in the usernames sent to a RADIUS server.

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple expert
[Device-radius-2000] key accounting simple expert
[Device-radius-2000] user-name-format with-domain
[Device-radius-2000] quit
```

3. Configure an ISP domain and specify the authentication, authorization, and accounting methods for users in the domain.

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

4. Configure a time range named **ftp** that contains a time span from 8:00 to 18:00 on weekdays.

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

5. Configure ACL 3000 to deny packets destined for the FTP server at 10.0.0.1 during the specified time span.

```
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-ipv4-adv-3000] quit
```

6. Configure 802.1X:

   # Enable 802.1X on interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

   # Enable 802.1X globally.

```
[Device] dot1x
```

Configuring the 802.1X client

Configure the 802.1X client. Make sure the client is able to update its IP address after the access port is assigned to the 802.1X guest VLAN or an authorization VLAN. (Details not shown.)

Verifying the configuration

Use the user account to pass authentication. (Details not shown.)

Verify that the user cannot ping the FTP server at any time from 8:00 to 18:00 on any weekday.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
```

```
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The output shows that ACL 3000 is active on the user, and the user cannot access the FTP server.

Configuration files

```
#
 time-range ftp 8:00 to 18:00 working-day
#
radius scheme 2000
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 key authentication cipher  $c$3$LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
 key accounting cipher $c$3 $LAV0oGNaM9Z/CuVcWONBH4xezu48Agh5aQ==
#
domain bbb
 authentication lan-access radius-scheme 2000
 authorization lan-access radius-scheme 2000
 accounting lan-access radius-scheme 2000
#
acl advanced 3000
 rule 0 deny ip destination 10.0.0.1 0 time-range ftp
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
 dot1x
#
```

Contents

Introduction

The following information provides examples for configuring MAC authentication to ensure network access security.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of MAC authentication.

Example: Configuring local MAC authentication

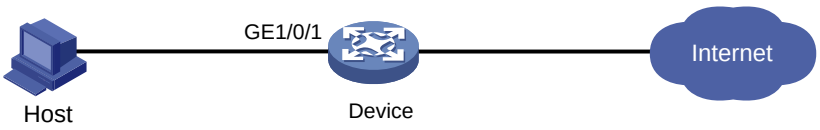
Network configuration

As shown in Figure 1, the device performs local MAC authentication on GigabitEthernet 1/0/1 to control Internet access of users.

Configure the device to meet the following requirements:

- Detect whether a user has gone offline every 180 seconds.
- Deny a user for 180 seconds if the user fails MAC authentication.
- Authenticate all users in ISP domain **bbb**.
- Use the MAC address of each user as both the username and password for authentication. The MAC addresses are in hexadecimal notation with hyphens, and letters are in lower case. In this example, both the username and password are 08-00-27-00-98-d2.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx, Release 65xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the	Release 63xx

Hardware	Software version
S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

- To avoid valid users from being blocked, do not enable MAC authentication globally before you finish all settings.
- When you create a local user, the username and password must match the user account policy for MAC authentication. If MAC-based accounts are used, make sure the username and password of each user account are the same as the MAC address of the corresponding MAC authentication user.

Procedures

Add a network access user, set both the username and password to the MAC address of the host, and allow the user to use the LAN access service.

```
<Device> system-view
[Device] local-user 08-00-27-00-98-d2 class network
[Device-luser-network-08-00-27-00-98-d2] password simple 08-00-27-00-98-d2
[Device-luser-network-08-00-27-00-98-d2] service-type lan-access
[Device-luser-network-08-00-27-00-98-d2] quit
```

Configure ISP domain **bbb** to use local authentication for LAN users.

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

Specify ISP domain **bbb** as the global MAC authentication domain.

```
[Device] mac-authentication domain bbb
```

Configure MAC authentication timers.

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

Use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation with hyphens, and letters are in lower case.

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication on interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

Enable MAC authentication globally.

```
[Device] mac-authentication
```

Verifying the configuration

IMPORTANT:

Support for VSI- and microsegment-related fields depends on the device model.

Display MAC authentication settings and statistics.

```
<Device> display mac-authentication
 Global MAC authentication parameters:
   MAC authentication                        : Enabled
   Authentication method                     : PAP
   Username format                           : MAC address in lowercase(xx-xx-xx-xx-
xx-xx)
            Username                         : mac
            Password                         : Not configured
   MAC range accounts                        : 0
          MAC address          Mask                 Username
   Offline detect period                     : 180 s
   Quiet period                              : 180 s
```

```
  Server timeout                            : 100 s
  Reauth period                             : 3600 s
  User aging period for critical VLAN       : 1000 s
  User aging period for critical VSI        : 1000 s
  User aging period for guest VLAN          : 1000 s
  User aging period for guest VSI           : 1000 s
  User aging period for critical microsegment: 1000 s
  Authentication domain                     : bbb
  HTTP proxy port list                      : Not configured
  HTTPS proxy port list                     : Not configured
Online MAC-auth wired users                 : 1
Silent MAC users:
         MAC address       VLAN ID  From port               Port index
GigabitEthernet1/0/1  is link-up
  MAC authentication              : Enabled
  Carry User-IP                   : Disabled
  Authentication domain           : Not configured
  Auth-delay timer                : Disabled
  Periodic reauth                 : Disabled
  Re-auth server-unreachable      : Logoff
  Guest VLAN                      : Not configured
  Guest VLAN reauthentication     : Enabled
    Guest VLAN auth-period        : 30 s
  Critical VLAN                   : Not configured
  Critical voice VLAN             : Disabled
  Host mode                       : Single VLAN
  Offline detection               : Enabled
  Authentication order            : Default
  User aging                      : Enabled
  Server-recovery online-user-sync : Disabled
  Guest VSI                       : Not configured
  Guest VSI reauthentication      : Enabled
    Guest VSI auth-period         : 30 s
  Critical VSI                    : Not configured
  Critical microsegment ID        : Not configured
  URL user logoff                 : No
  Auto-tag feature                : Disabled
  VLAN tag configuration ignoring  : Disabled
  Max online users                : 4294967295
  Authentication attempts         : successful 1, failed 0
  Current online users            : 1
         MAC address       Auth state
         0800-2700-98d2    Authenticated
```

Configuration files

```
#
 mac-authentication
```

```
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain bbb
 mac-authentication user-name-format mac-address with-hyphen lowercase
#
domain bbb
 authentication lan-access local
#
local-user 08-00-27-00-98-d2 class network
 password cipher $c$3$rTXB/eL1h+bXc/t2nyQOrhDMC0PWfyiPb93BqMCK+JFYwvn5
 service-type lan-access
 authorization-attribute user-role network-operator
#
interface GigabitEthernet1/0/1
mac-authentication
#
```

Example: Configuring MAC authentication with authorization VSI assignment

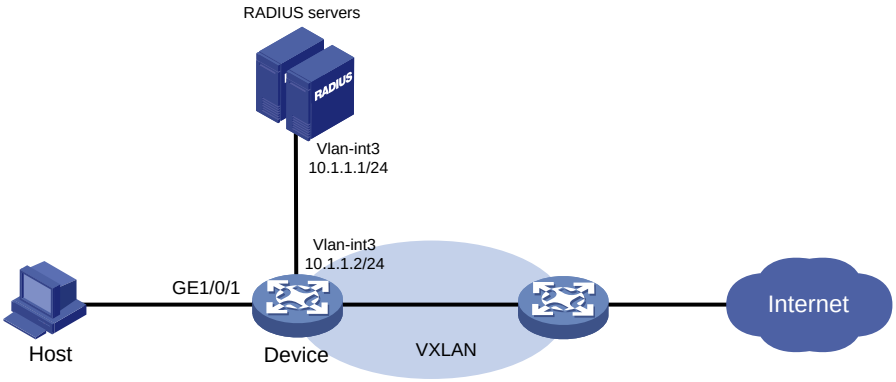
Network configuration

As shown in Figure 2:

- Configure the device to use the RADIUS servers to perform authentication, authorization, and accounting for the user on the host that is connected to GigabitEthernet 1/0/1.
- Enable MAC authentication on GigabitEthernet 1/0/1 to control Internet access.
- Configure the RADIUS servers to assign VSI **bbb** to the user when the user passes MAC authentication. After that, the user can access resources in the VXLAN created on the VSI. In this example, the VXLAN is VXLAN 5.
- Authenticate the user in ISP domain **2000**.
- Use the MAC address of the host as both the username and password for MAC authentication. The MAC address is in hexadecimal notation with hyphens, and letters are in lower case. In this example, both the username and password are d4-85-64-be-c6-3e.

IMC acts as the RADIUS servers.

Figure 2 Network diagram



Analysis

- For the device to use IMC as the RADIUS servers for user authentication, authorization, and accounting, perform the following tasks on IMC:
  a. Add the device to IMC as an access device.
  b. Add an access policy.
  c. Add an access service and specify the access policy in the access service.
  d. Add an access user and specify the access service for the access user.
- For the device to perform RADIUS-based authentication, authorization, and accounting for the MAC authentication access user, configure AAA settings on the device, including ISP domain settings and RADIUS scheme settings.
- To assign a VSI to the user after the user passes authentication and allow the user to access resources in the VXLAN created on the VSI, perform the following tasks:
  - On IMC, specify the VSI for the user when you add an access policy for the user.
  - On the device, create the VSI and its VXLAN.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series	Not supported

Hardware	Software version
S3100V3-SI switch series	
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

- To avoid valid users from being blocked, do not enable MAC authentication globally before you finish all settings.
- When you add an access user on IMC, make sure the user account on IMC matches the MAC authentication user account policy on the device. If MAC-based accounts are used, make sure the username and password of each user account are the same as the MAC address of the corresponding MAC authentication user.
- In standard RADIUS protocol, the authentication port on RADIUS servers is UDP port 1812. If an H3C device is used as a RADIUS server, the authentication port on the RADIUS server is UDP port 1645.

Procedures

If an ADCAM server is used for authentication and authorization, configure VSIs on the server. The server will assign these VSIs to the device. You do not need to configure VSIs on the device.

Configuring the RADIUS server

This example uses IMC PLAT 7.3 (E0506), IMC EIA 7.3 (E0503), and IMC EIP 7.3 (E0503) to describe the procedure.

Adding the device to the IMC Platform as an access device

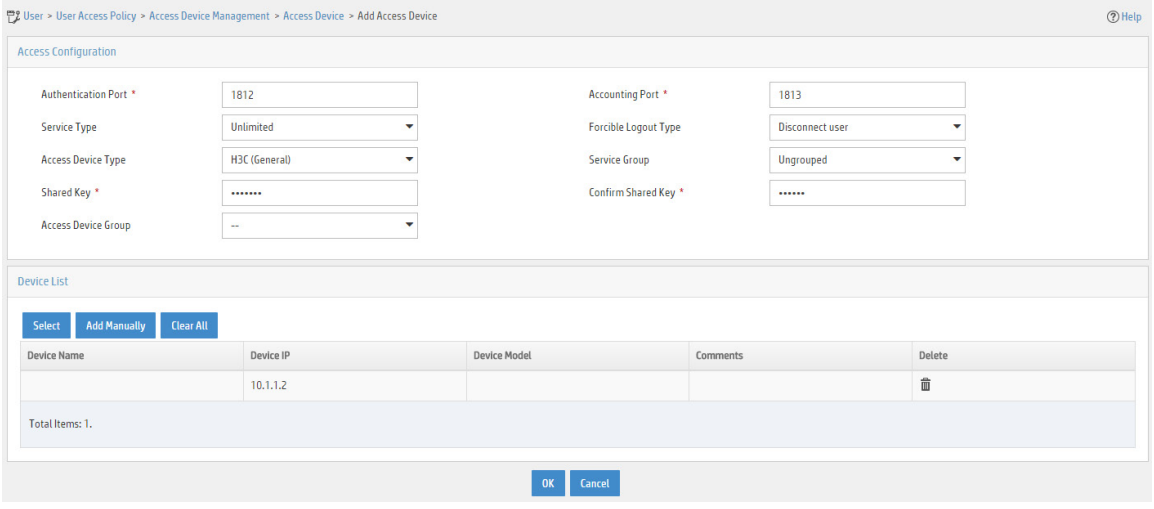
1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.
4. Click **Add**.
5. On the page that opens, configure access device parameters.
   a. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   b. Select **H3C (General)** from the **Access Device Type** list.
   c. Set the shared key to **expert** for secure authentication and accounting communication.
   d. Select an access device from the device list or manually add an access device. In this example, the IP address of the access device is 10.1.1.2.
   e. Use the default values for other parameters.
   f. Click **OK**.

   The IP address of the access device specified on IMC must be the same as the source IP address of the RADIUS packets sent from the device. On the device, the source IP address is chosen in the following order:

   a. IP address specified by using the **`nas-ip`** command.
   b. IP address specified by using the **`radius nas-ip`** command.
   c. IP address of the outbound interface (the default).

   In this example, the device uses the IP address of the outbound interface as the source IP address of RADIUS packets.

Figure 3 Adding an access device

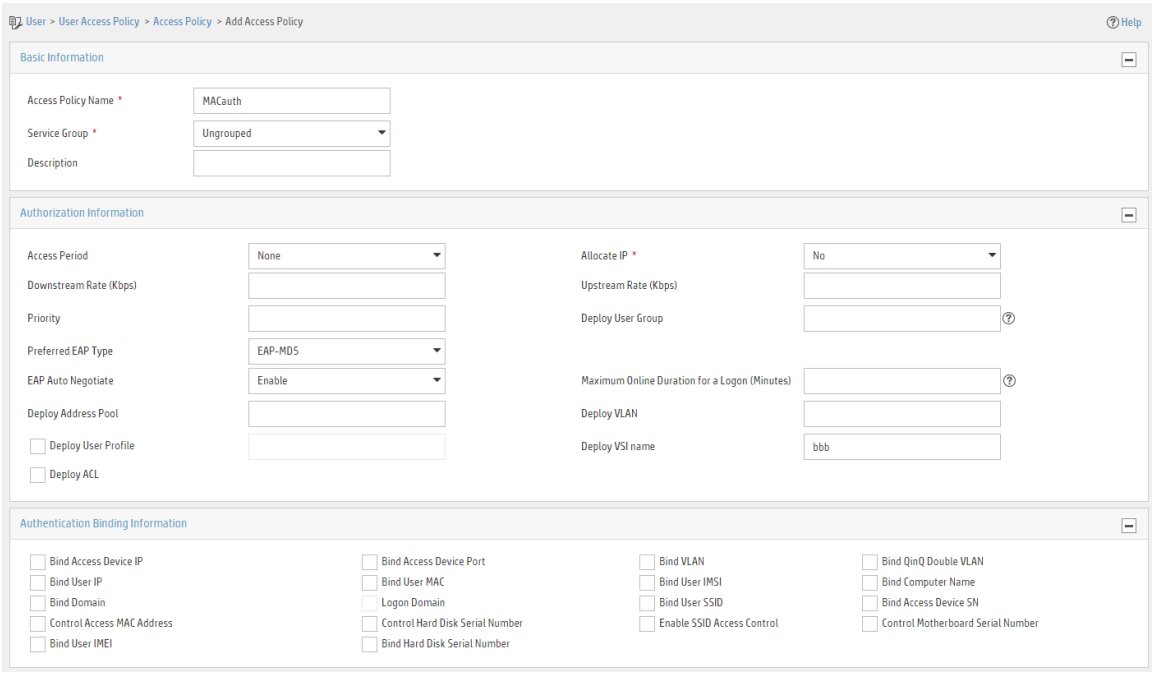


Adding an access policy

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Policy**.
3. Click **Add**.

4. On the page that opens, configure access policy parameters.
   a. Enter access policy name **MACauth**.
   b. Set the name of the VSI to be deployed to **bbb**.
   c. Configure other parameters as needed.
   d. Click **OK**.

Figure 4 Adding an access policy



Adding an access service

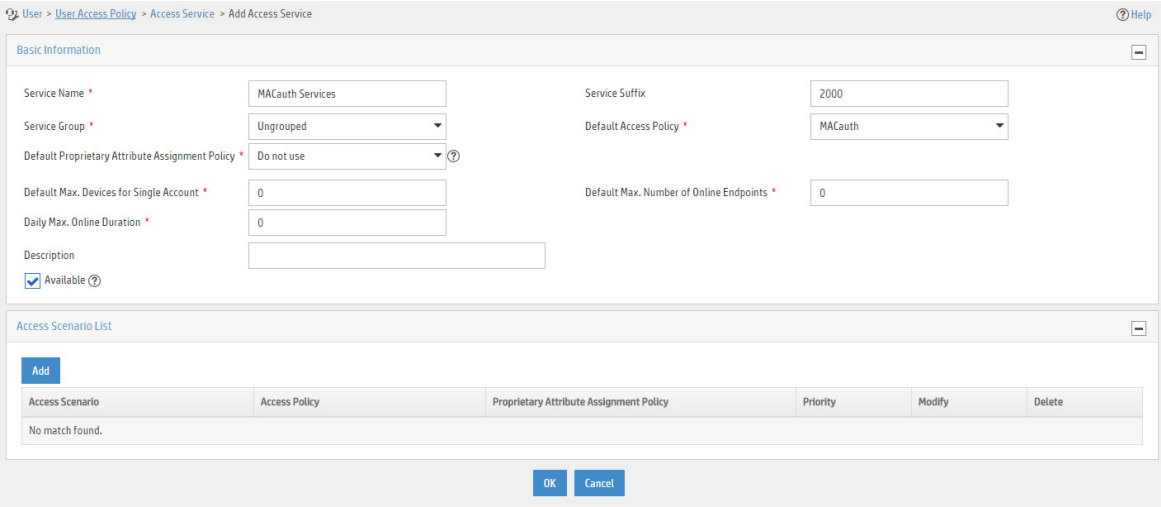
1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Service**.
3. Click **Add**.
4. On the page that opens, configure access service parameters.
   a. Enter service name **MACauth Service** and set the service suffix to **2000**. The service suffix is the authentication domain for the MAC authentication user.

   IMPORTANT:

   With the service suffix configured, you must configure the device to send usernames that include the domain name to the RADIUS servers.

   b. Select **MACauth** from the **Default Access Policy** list.
   c. Configure other parameters as needed.
   d. Click **OK**.

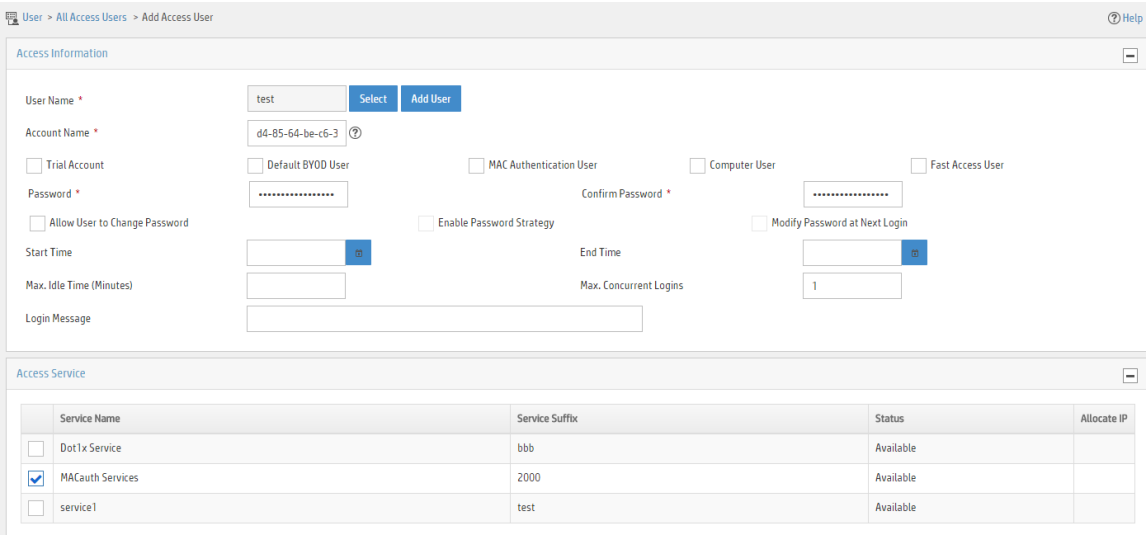
Figure 5 Adding an access service



Adding an access user

1. Click the **User** tab.
2. From the navigation pane, select **Access User** > **Access User**.
3. Click **Add**.
4. On the page that opens, configure access user parameters.
   a. Select the user or add a user named **test**.
   b. Enter account name **d4-85-64-be-c6-3e** and password **d4-85-64-be-c6-3e**.
   c. Select **MACauth Service** in the **Access Service** area.
   d. Configure other parameters as needed.
   e. Click **OK**.

Figure 6 Adding an access user



Configuring the device

Configure a RADIUS scheme.

IMPORTANT:

With the service suffix configured on IMC, you must configure the device to send usernames that include the domain name to the RADIUS servers. By default, the device includes the domain name in the usernames sent to a RADIUS server.

```
<Device> system-view
[Device] radius scheme bbb
[Device-radius-bbb] primary authentication 10.1.1.1
[Device-radius-bbb] primary accounting 10.1.1.2
[Device-radius-bbb] key authentication simple expert
[Device-radius-bbb] key accounting simple expert
[Device-radius-bbb] user-name-format with-domain
[Device-radius-bbb] quit
```

Configure ISP domain **2000**.

```
[Device] domain 2000
[Device-isp-2000] authentication lan-access radius-scheme bbb
[Device-isp-2000] authorization lan-access radius-scheme bbb
[Device-isp-2000] accounting lan-access radius-scheme bbb
[Device-isp-2000] quit
```

Enable MAC authentication on interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
```

Enable MAC-based traffic match mode for dynamic Ethernet service instances on interface GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] mac-based ac
[Device-GigabitEthernet1/0/1] quit
```

Enable L2VPN.

```
[Device] l2vpn enable
```

Create a VSI named **bbb** and the associated VXLAN.

```
[Device] vsi bbb
[Device-vsi-bbb] vxlan 5
[Device-vsi-bbb-vxlan-5] quit
[Device-vsi-bbb] quit
```

Specify ISP domain **2000** as the global MAC authentication domain.

```
[Device] mac-authentication domain 2000
```

Use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation with hyphens, and letters are in lower case.

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication globally.

```
[Device] mac-authentication
```

Verifying the configuration

Verify that VSI **bbb** is assigned to the MAC authentication user after the user passes authentication.

```
[Device] display mac-authentication connection
Total connections: 1
```

```
Slot ID: 1
User MAC address: d485-64be-c63e
Access interface: GigabitEthernet1/0/1
Username: d4-85-64-be-c6-3e
User access state: Successful
Authentication domain: 2000
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: N/A
Authorization tagged VLAN: N/A
Authorization VSI: bbb
Authorization microsegment ID: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
Authorization CAR:
  Average input rate: 102400 bps
  Peak input rate: 204800 bps
  Average output rate: 102400 bps
  Peak output rate: 204800 bps
Authorization URL: N/A
Termination action: N/A
Session timeout period: N/A
Offline detection: 100 sec (server-assigned)
Online from: 2016/06/13 09:06:37
Online duration: 0h 0m 35s
```

Verify that a dynamic AC is created for MAC address **d485-64be-c63e**.

```
[Device] display l2vpn forwarding ac verbose
VSI Name: bbb
  Interface: GE1/0/1  Service Instance: 1
    Link ID      : 0
    Access Mode  : VLAN
    Encapsulation: untagged
    Type         : Dynamic (MAC-based)
    MAC address  : d485-64be-c63e
```

Configuration files

```
#
radius scheme bbb
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 key authentication cipher $c$3$+zuETC3Y0LHiW3bxzBb+UNEuWlxHkQ==
 key accounting cipher $c$3$2b8hx6mbWlnMMQY82TeUzgh0VnWXbg==
#
domain 2000
 authentication lan-access radius-scheme bbb
 accounting lan-access radius-scheme bbb
```

```
#
interface GigabitEthernet1/0/1
 mac-authentication
 mac-based ac
#
vsi bbb
 vxlan 5
#
 l2vpn enable
#
 mac-authentication domain 2000
#
 mac-authentication user-name-format mac-address with-hyphen lowercase
#
 mac-authentication
#
```

Example: Configuring MAC authentication with ACL assignment

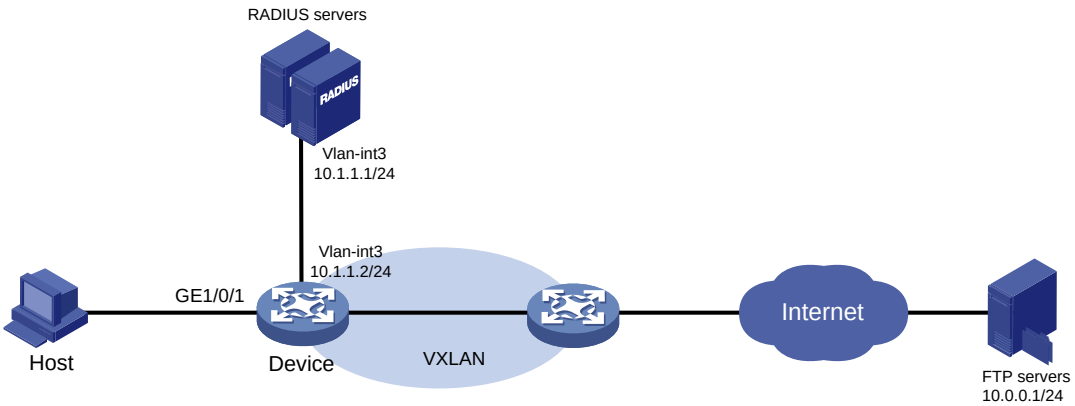
Network configuration

As shown in Figure 7:

- Configure the device to use the RADIUS servers to perform authentication, authorization, and accounting for the user on the host that is connected to GigabitEthernet 1/0/1.
- Enable MAC authentication on GigabitEthernet 1/0/1 to control Internet access.
- Use the MAC address of the host as both the username and password for MAC authentication. The MAC address is in hexadecimal notation with hyphens, and letters are in lower case.
- Use an ACL to deny the user to access the FTP server at 10.0.0.1 after the user passes authentication.

IMC acts as the RADIUS servers.

Figure 7 Network diagram



Analysis

- For the device to use IMC as the RADIUS servers for user authentication, authorization, and accounting, perform the following tasks on IMC:
  a. Add the device to IMC as an access device.
  b. Add an access policy.
  c. Add an access service and specify the access policy in the access service.
  d. Add an access user and specify the access service for the access user.
- For the device to perform RADIUS-based authentication, authorization, and accounting for the MAC authentication access user, configure AAA settings on the device, including ISP domain settings and RADIUS scheme settings.
- To use an ACL to restrict the user's network access behaviors after the user passes authentication, perform the following tasks:
  - On IMC, specify the ACL number for the user when you add an access policy for the user.
  - On the device, create the ACL and configure its rules.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

- To avoid valid users from being blocked, do not enable MAC authentication globally before you finish all settings.
- When you add an access user on IMC, make sure the user account on IMC matches the MAC authentication user account policy on the device. If MAC-based accounts are used, make sure the username and password of each user account are the same as the MAC address of the corresponding MAC authentication user.
- In standard RADIUS protocol, the authentication port on RADIUS servers is UDP port 1812. If an H3C device is used as a RADIUS server, the authentication port on the RADIUS server is UDP port 1645.

Procedures

Configuring the RADIUS server

This example uses IMC PLAT 7.3 (E0506), IMC EIA 7.3 (E0503), and IMC EIP 7.3 (E0503) to describe the procedure.

Adding the device to the IMC Platform as an access device

1. Log in to IMC.
2. Click the **User** tab.
3. From the navigation pane, select **User Access Policy** > **Access Device Management** > **Access Device**.
4. Click **Add**.
5. On the page that opens, configure access device parameters.
   a. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   b. Select **H3C (General)** from the **Access Device Type** list.

c. Set the shared key to **expert** for secure authentication and accounting communication.

d. Select an access device from the device list or manually add an access device. In this example, the IP address of the access device is 10.1.1.2.

e. Use the default values for other parameters.

f. Click **OK**.

The IP address of the access device specified on IMC must be the same as the source IP address of the RADIUS packets sent from the device. On the device, the source IP address is chosen in the following order:

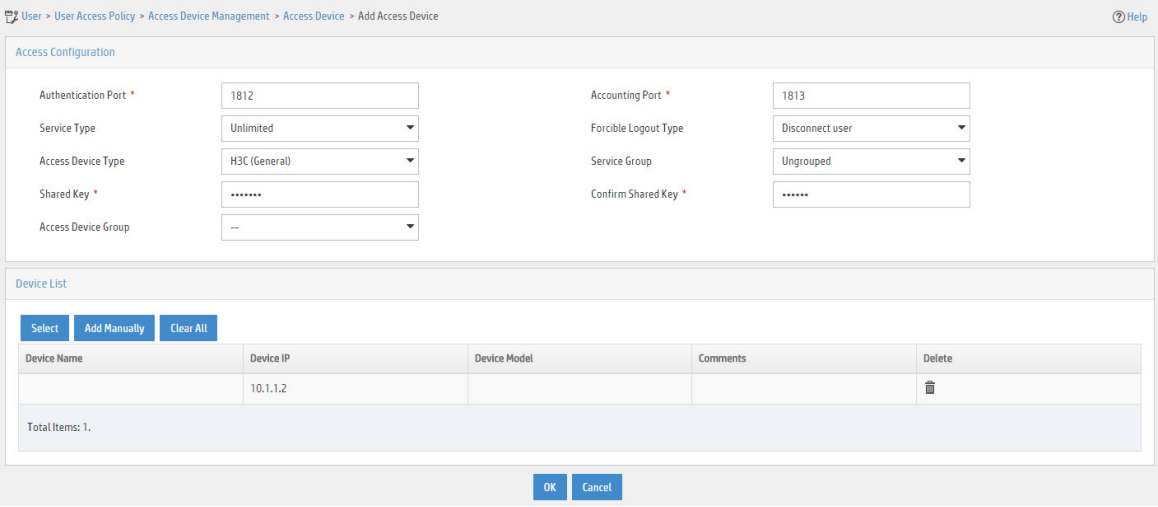
a. IP address specified by using the **`nas-ip`** command.

b. IP address specified by using the **`radius nas-ip`** command.

c. IP address of the outbound interface (the default).

In this example, the device uses the IP address of the outbound interface as the source IP address of RADIUS packets.

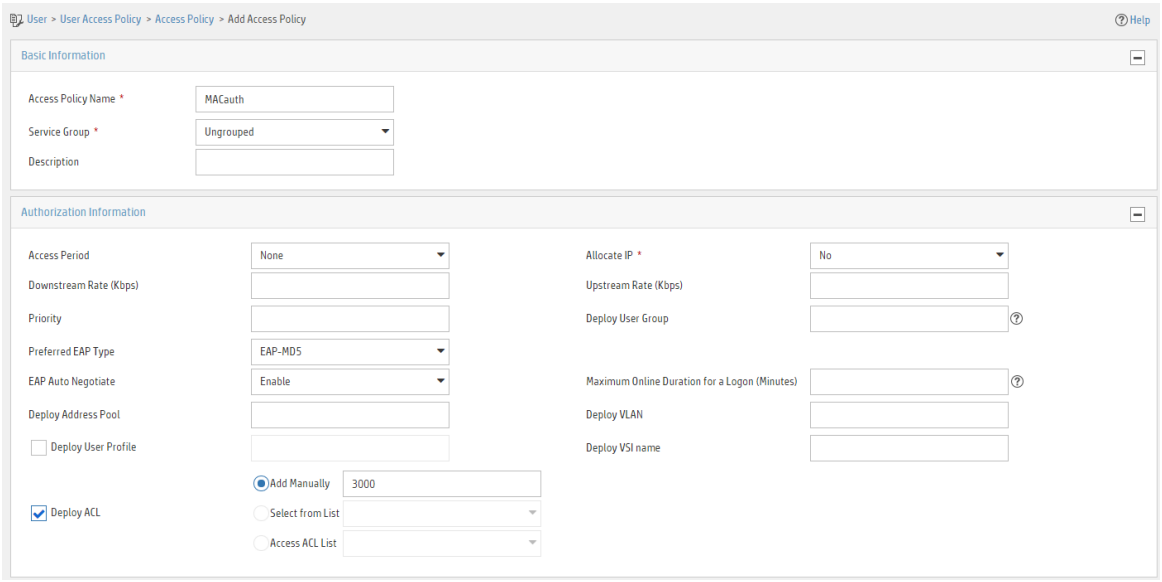
Figure 8 Adding an access device



Adding an access policy

1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Policy**.
3. Click **Add**.
4. On the page that opens, configure access policy parameters.
   a. Enter access policy name **MACauth**.
   b. Select **Deploy ACL** and manually enter ACL number **3000**.
   c. Configure other parameters as needed.
   d. Click **OK**.

Figure 9 Adding an access policy



Adding an access service

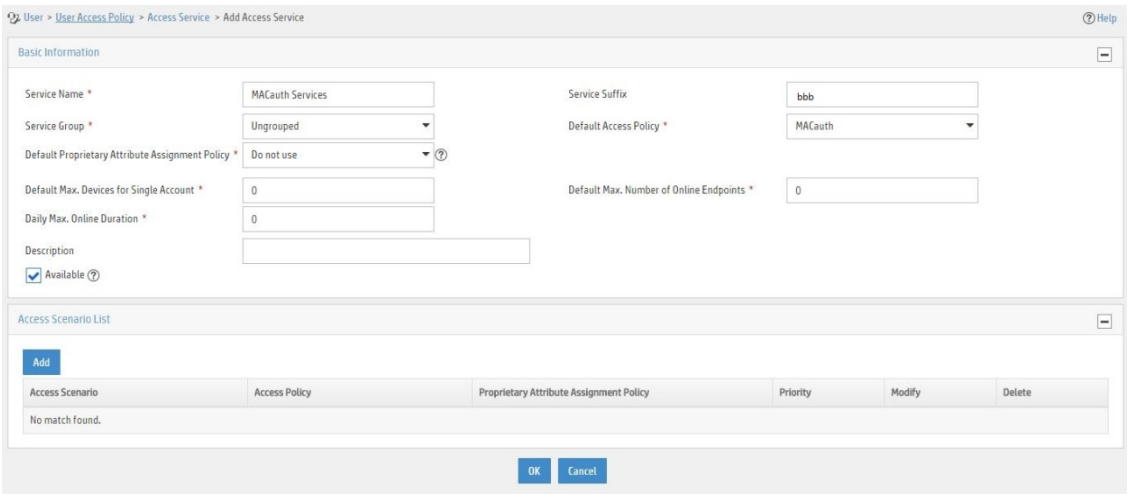
1. Click the **User** tab.
2. From the navigation pane, select **User Access Policy** > **Access Service**.
3. Click **Add**.
4. On the page that opens, configure access service parameters.
   a. Enter service name **MACauth Services** and set the service suffix to **bbb**. The service suffix is the authentication domain for the MAC authentication user.

   IMPORTANT:

   With the service suffix configured, you must configure the device to send usernames that include the domain name to the RADIUS servers.

   b. Select **MACauth** from the **Default Access Policy** list.
   c. Configure other parameters as needed.
   d. Click **OK**.

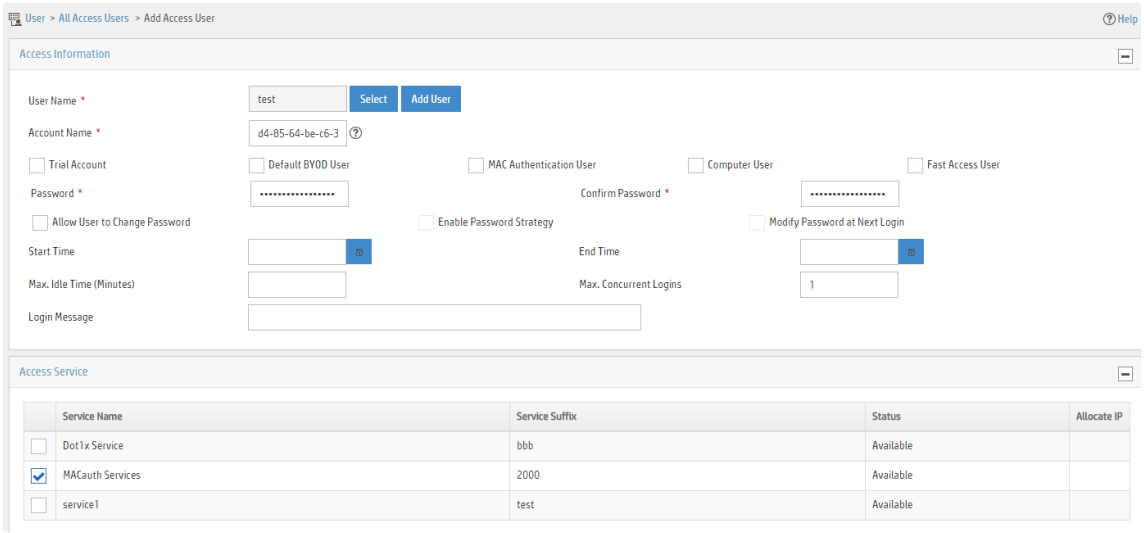
Figure 10 Adding an access service



Adding an access user

1. Click the **User** tab.
2. From the navigation pane, select **Access User** > **Access User**.
3. Click **Add**.
4. On the page that opens, configure access user parameters.
   a. Select the user or add a user named **test**.
   b. Enter account name **d4-85-64-be-c6-3e** and password **d4-85-64-be-c6-3e**.
   c. Select **MACauth Services** in the **Access Service** area.
   d. Configure other parameters as needed.
   e. Click **OK**.

Figure 11 Adding an access user



Configuring the device

1. Configure advanced ACL 3000 to deny packets destined for 10.0.0.1.

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Device-acl-ipv4-adv-3000] quit
```

2. Configure RADIUS-based MAC authentication:

   # Configure a RADIUS scheme.

IMPORTANT:

With the service suffix configured on IMC, you must configure the device to send usernames that include the domain name to the RADIUS servers. By default, the device includes the domain name in the usernames sent to a RADIUS server.

```
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple expert
[Device-radius-2000] key accounting simple expert
```

```
[Device-radius-2000] user-name-format with-domain
[Device-radius-2000] quit
```

Create ISP domain **bbb** and configure the ISP domain to use RADIUS scheme **2000** for user authentication, authorization, and accounting.

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

Specify ISP domain **bbb** as the global MAC authentication domain.

```
[Device] mac-authentication domain bbb
```

Use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation with hyphens, and letters are in lower case.

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Enable MAC authentication on interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

Enable MAC authentication globally.

```
[Device] mac-authentication
```

Verifying the configuration

IMPORTANT:

Support for VSI- and microsegment-related fields depends on the device model.

Display MAC authentication settings and statistics.

```
<Device> display mac-authentication
 Global MAC authentication parameters:
   MAC authentication                          : Enable
   Authentication method                       : PAP
   DR member configuration conflict            : Unknown
   Username format                             : MAC address in lowercase(xx-xx-xx-xx-
xx-xx)
            Username                           : mac
            Password                           : Not configured
   MAC range accounts                  : 0
          MAC address          Mask                 Username
   Offline detect period                       : 300 s
   Quiet period                                : 60 s
   Server timeout                              : 100 s
   Reauth period                               : 3600 s
   User aging period for critical VLAN         : 1000 s
   User aging period for critical VSI          : 1000 s
   User aging period for guest VLAN            : 1000 s
   User aging period for guest VSI             : 1000 s
   User aging period for critical microsegment: 1000 s
```

```
  Temporary user aging period         : 60 s
  Authentication domain                      : bbb
  HTTP proxy port list                       : Not configured
  HTTPS proxy port list                      : Not configured
Online MAC-auth wired users                  : 1

Silent MAC users:
         MAC address       VLAN ID  From port               Port index

GigabitEthernet1/0/1  is link-up
  MAC authentication               : Enabled
  Carry User-IP                    : Disabled
  Authentication domain            : Not configured
  Auth-delay timer                 : Disabled
  Periodic reauth                  : Disabled
  Re-auth server-unreachable       : Logoff
  Guest VLAN                       : Not configured
  Guest VLAN reauthentication      : Enabled
    Guest VLAN auth-period         : 30 s
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Host mode                        : Single VLAN
  Offline detection                : Enabled
  Authentication order             : Default
  User aging                       : Enabled
  Server-recovery online-user-sync : Enabled

  Guest VSI                        : Not configured
  Guest VSI reauthentication       : Enabled
    Guest VSI auth-period          : 30 s
  Critical VSI                     : Not configured
  Critical microsegment ID         : Not configured
  URL user logoff                  : No
  Auto-tag feature                 : Disabled
  VLAN tag configuration ignoring  : Disabled
  Max online users                 : 4294967295
  Authentication attempts          : successful 1, failed 0
  Current online users             : 1
         MAC address       Auth state
         0800-2712-3456    Authenticated
```

Verify that you cannot ping the FTP server from the host.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

```
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

The output shows that ACL 3000 has been assigned to GigabitEthernet 1/0/1 to deny access to the FTP server.

Configuration files

```
#
acl advanced 3000
 rule 0 deny ip destination 10.0.0.1 0
#
 radius scheme 2000
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 key authentication cipher $c$3$PJM7Px3rbC96Kvh8RyFWHMLatExagQ==
 key accounting cipher $c$3$rr7AO7ZuSNZ+b+deWrfb/Qg1JPc97g==
#
 domain bbb
 authentication default radius-scheme 2000
 authorization default radius-scheme 2000
 accounting  default radius-scheme 2000
#
 mac-authentication domain bbb
#
 mac-authentication user-name-format mac-address with-hyphen lowercase
#
interface GigabitEthernet1/0/1
 mac-authentication
#
 mac-authentication
#
```

Contents

Introduction

This document provides examples for configuring an ISATAP tunnel and a 6to4 tunnel.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of ISATAP tunneling and 6to4 tunneling.

Example: Configuring an ISATAP tunnel and a 6to4 tunnel

Network configuration

As shown in Figure 1, configure a 6to4 tunnel between Device A and Device B to allow communications between the headquarters and the branches over the IPv4 network.

Configure an ISATAP tunnel between Device A and the ISATAP host to allow the host in the IPv4 network to access the headquarters.

Figure 1 Network diagram

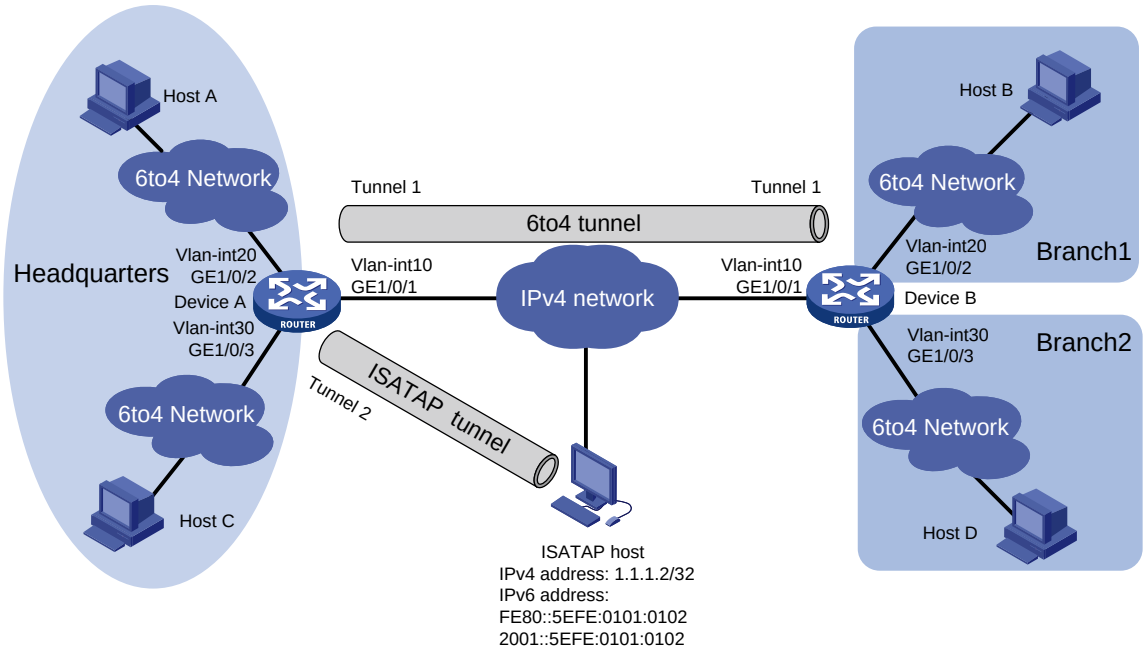


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int10	2.1.1.1/24	Device B	Vlan-int10	3.1.1.1/24

Device	Interface	IP address	Device	Interface	IP address
	Vlan-int20	2002:0201:0101:1::1/64		Vlan-int20	2002:0301:0101:1::1/64
	Vlan-int30	2002:0201:0101:2::1/64		Vlan-int30	2002:0301:0101:2::1/64
	Tunnel 1	3001::1/64		Tunnel 1	3001::2/64
	Tunnel 2	2001::5EFE:0201:0101/64			

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported

S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx switch series

Restrictions and guidelines

When you configure an ISATAP tunnel and a 6to4 tunnel, follow these restrictions and guidelines:

- You do not need to configure a destination address for a 6to4 tunnel, because the destination IPv4 address is embedded in the 6to4 IPv6 address whose format is 2002:IPv4-destination-address::/64.
- You do not need to configure a destination address for an ISATAP tunnel, because the destination IPv4 address is embedded in the ISATAP address whose format is Prefix:0:5EFE:IPv4-destination-address.
- Disable RA suppression on Device A and Device B to allow hosts to acquire address prefixes automatically. This configuration ensures that hosts in the same network use the same address prefix.

  After RA suppression is disabled, the ISATAP host and hosts in the headquarters acquire address prefixes from RA messages advertised by Device A. Hosts in the branches acquire address prefixes from RA messages advertised by Device B.

Procedures

Make sure Device A and Device B can reach each other through IPv4.

Configuring Device A

Configure an IP address for VLAN-interface 10.

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port GigabitEthernet 1/0/1
[DeviceA-vlan10] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 2.1.1.1 24
[DeviceA-Vlan-interface10] quit
```

Configure IP addresses for other interfaces as shown in Table 1. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/4 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceA] service-loopback group 1 type tunnel
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port service-loopback group 1
[DeviceA-GigabitEthernet1/0/4] quit
```

Create a 6to4 tunnel interface Tunnel 1.

```
[DeviceA] interface tunnel 1 mode ipv6-ipv4 6to4
```

Specify an IPv6 address for the tunnel interface.

```
[DeviceA-Tunnel1] ipv6 address 3001::1/64
```

Specify the source interface as VLAN-interface 10 for the tunnel interface.

```
[DeviceA-Tunnel1] source vlan-interface 10
[DeviceA-Tunnel1] quit
```

Configure a static route destined for 2002:0301:0101::/48 through the tunnel interface.

```
[DeviceA] ipv6 route-static 2002:0301:0101:: 48 tunnel 1
```

Create an ISATAP tunnel interface Tunnel 2.

```
[DeviceA] interface tunnel 2 mode ipv6-ipv4 isatap
```

Specify an IPv6 address for the tunnel interface.

```
[DeviceA-Tunnel2] ipv6 address 2001::5EFE:0201:0101 64
```

Specify the source interface as VLAN-interface 10 for the tunnel interface.

```
[DeviceA-Tunnel2] source  vlan-interface 10
[DeviceA-Tunnel2] quit
```

Configure a static route destined for 2001::/16 through the tunnel interface.

```
[DeviceA] ipv6 route-static 2001:: 16 tunnel 2
```

Disable RA suppression.

```
[DeviceA] interface Tunnel 2
[DeviceA-Tunnel2] undo ipv6 nd ra halt
[DeviceA-Tunnel2] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] undo ipv6 nd ra halt
[DeviceA-Vlan-interface20] quit
[DeviceA] interface  vlan-interface 30
[DeviceA-Vlan-interface30] undo ipv6 nd ra halt
[DeviceA-Vlan-interface30] quit
```

Configuring Device B

Configure an IP address for VLAN-interface 10.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port GigabitEthernet 1/0/1
[DeviceB-vlan10] quit
[DeviceB] interface  vlan-interface 10
[DeviceB-Vlan-interface10] ip address 3.1.1.1 24
[DeviceB-Vlan-interface10] quit
```

Configure IP addresses for other interfaces as shown in Table 1. (Details not shown.)

Create service loopback group 1 and specify tunnel services for the group, and then add GigabitEthernet 1/0/4 to the group. (This step is required for the S6550XE-HI, S6525XE-HI, S5850, and IE4520 switch series to receive and send tunnel packets.)

```
[DeviceB] service-loopback group 1 type tunnel
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port service-loopback group 1
[DeviceB-GigabitEthernet1/0/4] quit
```

Create a 6to4 tunnel interface Tunnel 1.

```
[DeviceB] interface tunnel 1 mode ipv6-ipv4 6to4
```

Specify an IPv6 address for the tunnel interface.

```
[DeviceB-Tunnel1] ipv6 address 3001::2/64
```

Specify the source interface as VLAN-interface 10 for the tunnel interface.

```
[DeviceB-Tunnel1] source  vlan-interface 10
[DeviceB-Tunnel1] quit
```

Configure a static route destined for 2002:0201:0101::/48 through the tunnel interface.

```
[DeviceB] ipv6 route-static 2002:0201:0101:: 48 tunnel 1
```

Disable RA suppression.

```
[DeviceB] interface vlan-interface 20
[DeviceB-Vlan-interface20] undo ipv6 nd ra halt
[DeviceB-Vlan-interface20] quit
[DeviceB] interface vlan-interface 30
[DeviceB-Vlan-interface30] undo ipv6 nd ra halt
[DeviceB-Vlan-interface30] quit
```

Configuring the ISATAP host

Configurations on the ISATAP host vary by operating system. The following example is performed on Windows XP.

Install IPv6.

```
C:\>ipv6 install
```

Configure an ISATAP tunnel.

```
C:\>netsh interface ipv6 isatap set router 2.1.1.1
```

Display information about the ISATAP tunnel interface.

```
C:\>ipv6 if 2
Interface 2: Automatic Tunneling Pseudo-Interface
  Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
  does not use Neighbor Discovery
  uses Router Discovery
  routing preference 1
  EUI-64 embedded IPv4 address: 1.1.1.2
  router link-layer address: 2.1.1.1
    preferred global 2001::5efe:1.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
    preferred link-local fe80::5efe:1.1.1.2, life infinite
  link MTU 1500 (true link MTU 65515)
  current hop limit 255
  reachable time 42500ms (base 30000ms)
  retransmission interval 1000ms
  DAD transmits 0
  default site prefix length 48
```

The host has acquired the prefix 2001::/64 and has automatically generated the global unicast address 2001::5efe:1.1.1.2. The message "uses Router Discovery" indicates that the router discovery function is enabled on the host.

Display information about IPv6 routes on the host.

```
C:\>ipv6 rt
2001::/64 -> 2 pref 1if+8=9 life 29d23h59m43s (autoconf)
::/0 -> 2/fe80::5efe:1.1.1.1 pref 1if+256=257 life 29m43s (autoconf)
```

Verifying the configuration

Verify that Host A and Host B can ping each other.

```
D:\>ping6 -s 2002:0201:0101:1::2 2002:0301:0101:1::2
```

```
Pinging 2002:0301:0101:1::2
from 2002:0201:0101:1::2 with 32 bytes of data:

Reply from 2002:0301:0101:1::2: bytes=32 time=13ms
Reply from 2002:0301:0101:1::2: bytes=32 time=1ms
Reply from 2002:0301:0101:1::2: bytes=32 time=1ms
Reply from 2002:0301:0101:1::2: bytes=32 time<1ms

Ping statistics for 2002:0301:0101:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Verify that the ISATAP host can ping Host A.

```
C:\Documents and Settings\Administrator>pingv6 2002:0201:0101:1::2

Pinging 2002:0201:0101:1::2 with 32 bytes of data:

Reply from 2002:0201:0101:1::2: time=33ms
Reply from 2002:0201:0101:1::2: time=32ms
Reply from 2002:0201:0101:1::2: time=32ms
Reply from 2002:0201:0101:1::2: time=33ms

Ping statistics for 2002:0201:0101:1::2:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 32ms, Maximum = 33ms, Average = 32ms
```

Configuration files

- Device A:

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
vlan 30
#
interface Vlan-interface10
 ip address 2.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ipv6 address 2002:201:101:1::1/64
 undo ipv6 nd ra halt
#
interface Vlan-interface30
 ipv6 address 2002:201:101:2::1/64
```

```
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode ipv6-ipv4 6to4
 source Vlan-interface10
 ipv6 address 3001::1/64
#
interface Tunnel2 mode ipv6-ipv4 isatap
 source Vlan-interface10
 ipv6 address 2001::5EFE:201:101/64
 undo ipv6 nd ra halt
#
 ipv6 route-static 2001:: 16 Tunnel2
 ipv6 route-static 2002:301:101:: 48 Tunnel1
#
```

- Device B:

```
#
 service-loopback group 1 type tunnel
#
vlan 10
#
vlan 20
#
vlan 30
#
interface Vlan-interface10
 ip address 3.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ipv6 address 2002:301:101:1::1/64
 undo ipv6 nd ra halt
#
interface Vlan-interface30
```

```
 ipv6 address 2002:301:101:2::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel1 mode ipv6-ipv4 6to4
 source Vlan-interface10
 ipv6 address 3001::2/64
#
 ipv6 route-static 2002:201:101:: 48 Tunnel1
#
```

Contents

Introduction

This document introduces BIDIR-PIM configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of BIDIR-PIM.

Example: Configuring BIDIR-PIM

Network configuration

As shown in Figure 1:

- Switch A, Switch B, and Switch C run OSPF.
- Source 1 and Source 2 send multicast data to multicast group 225.1.1.1.
- Host A and Host B are member hosts of multicast group 225.1.1.1.

Configure BIDIR-PIM on the switches to implement multicast forwarding.

Figure 1 Network diagram

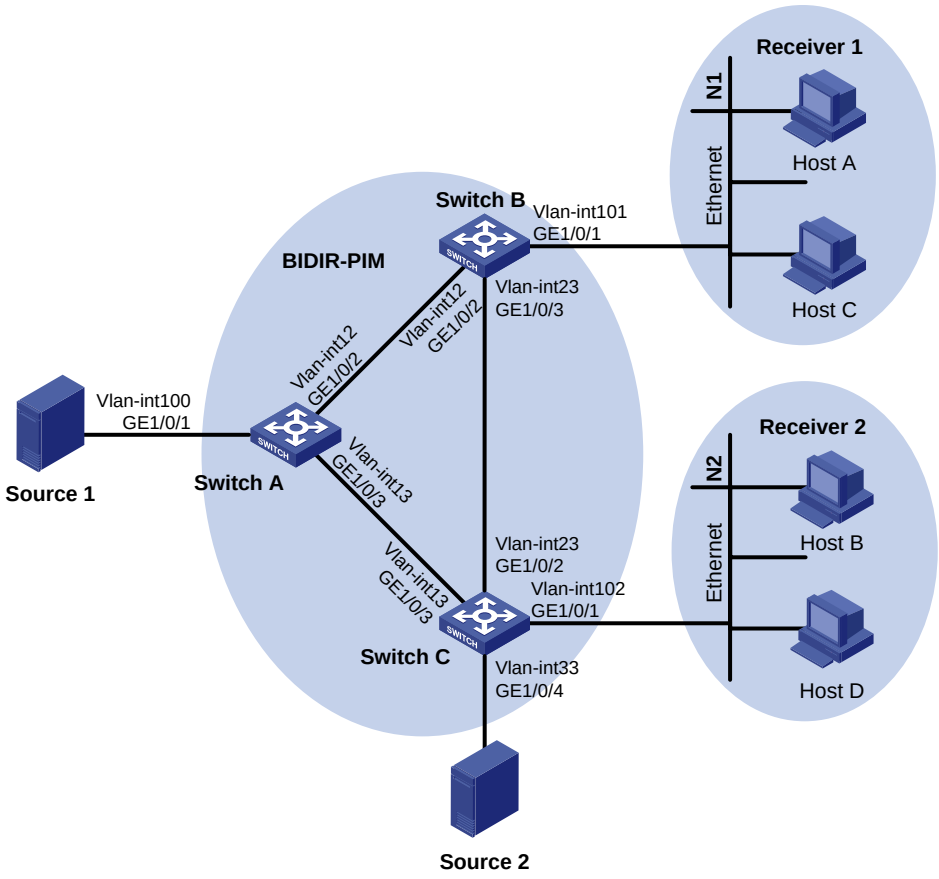


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.10.1.1/24	Switch C	Vlan-int102	10.102.1.1/24
Switch A	Vlan-int12	10.12.1.1/24	Switch C	Vlan-int13	10.13.1.3/24
Switch A	Vlan-int13	10.13.1.1/24	Switch C	Vlan-int23	10.23.1.3/24
Switch B	Vlan-int101	10.101.1.1/24	Switch C	Vlan-int33	10.33.1.3/24
Switch B	Vlan-int12	10.12.1.2/24	Source 1	—	10.10.1.2/24
Switch B	Vlan-int23	10.23.1.2/24	Source 2	—	10.33.1.4/24

Analysis

To meet the network requirements, perform the following tasks:

- To establish the bidirectional RPT, configure VLAN-interface 12 on Switch A as a C-RP.
- To use the BSR mechanism to dynamically elect the RP, configure VLAN-interface 12 on Switch A as a C-BSR.
- To avoid multicast forwarding interruption when the RP fails, specify the unused IP address 10.13.1.4/24 as the static RP. In this way, the link on the subnet 10.13.1.0/24 becomes the RPL. Switch A and Switch C on the link function as the RPs.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure BIDIR-PIM, follow these restrictions and guidelines:

- Enable the same PIM mode on the interfaces that belong to the same VPN instance on each switch.

- Configure the same static RP on all the switches in the BIDIR-PIM domain.
- Enable PIM-SM for all interfaces on the switches in the BIDIR-PIM domain.
- Enable IGMP for the interfaces that connect to the stub networks on all the switches in the BIDIR-PIM domain.

Procedures

Configure Switch A

1. Enable IP multicast routing.

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

2. Configure each interface and enable PIM-SM.

Create VLAN 100, and assign GigabitEthernet 1/0/1 to this VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
```

Assign an IP address to VLAN-interface 100, and enable PIM-SM on the interface.

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.10.1.1 24
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
```

Create VLAN 12, and assign GigabitEthernet 1/0/2 to the VLAN.

```
[SwitchA] vlan 12
[SwitchA-vlan12] port gigabitethernet 1/0/2
[SwitchA-vlan12] quit
```

Assign an IP address to VLAN-interface 12, enable PIM-SM on the interface.

```
[SwitchA-vlan12] interface vlan-interface 12
[SwitchA-Vlan-interface12] ip address 10.12.1.1 24
[SwitchA-Vlan-interface12] pim sm
[SwitchA-Vlan-interface12] quit
```

Create VLAN 13, and assign GigabitEthernet 1/0/3 to the VLAN.

```
[SwitchA] vlan 13
[SwitchA-vlan13] port gigabitethernet 1/0/3
[SwitchA-vlan13] quit
```

Assign an IP address to VLAN-interface 13, enable PIM-SM on the interface.

```
[SwitchA] interface vlan-interface 13
[SwitchA-Vlan-interface13] ip address 10.13.1.1 24
[SwitchA-Vlan-interface13] pim sm
[SwitchA-Vlan-interface13] quit
```

3. Configure a C-RP, a C-BSR, and the static RP.

Configure VLAN-interface 12 as a C-BSR and a C-RP.

```
[SwitchA] pim
[SwitchA-pim] c-bsr 10.12.1.1
[SwitchA-pim] c-rp 10.12.1.1 bidir
```

Specify the unused IP address 10.13.1.4 as a static RP.

```
[SwitchA-pim] static-rp 10.13.1.4 bidir
```

4. Enable BIDIR-PIM.

```
[SwitchA-pim] bidir-pim enable
[SwitchA-pim] quit
```

5. Configure OSPF.

```
[SwitchA] ospf 1
[SwitchA-ospf-1] import-route direct
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure Switch B

1. Enable IP multicast routing.

```
<SwitchB> system-view
System View: return to User View with Ctrl+Z.
[SwitchB] multicast routing
[SwitchB-mrib] quit
```

2. Configure each interface and enable PIM-SM.

Create VLAN 12, and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchB] vlan 12
[SwitchB-vlan12] port gigabitethernet 1/0/2
[SwitchB-vlan12] quit
```

Assign an IP address to VLAN-interface 12, enable PIM-SM on the interface.

```
[SwitchB] interface vlan-interface 12
[SwitchB-Vlan-interface12] ip address 10.12.1.2 24
[SwitchB-Vlan-interface12] pim sm
[SwitchB-Vlan-interface12] quit
```

Create VLAN 23, and assign GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchB] vlan 23
[SwitchB-vlan23] port gigabitethernet 1/0/3
[SwitchB-vlan23] quit
```

Assign an IP address to VLAN-interface 23, enable PIM-SM on the interface.

```
[SwitchB] interface vlan-interface 23
[SwitchB-Vlan-interface23] ip address 10.23.1.2 24
[SwitchB-Vlan-interface23] pim sm
[SwitchB-Vlan-interface23] quit
```

Create VLAN 101, and assign GigabitEthernet 1/0/1 to this VLAN.

```
[SwitchB] vlan 101
[SwitchB-vlan101] port gigabitethernet 1/0/1
[SwitchB-vlan101] quit
```

Assign an IP address to VLAN-interface 101, enable PIM-SM and IGMP on the interface.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 10.101.1.1 24
[SwitchB-Vlan-interface101] igmp enable
```

```
[SwitchB-Vlan-interface101] quit
```

3. Specify the unused IP address 10.13.1.4 as a static RP.

```
[SwitchB] pim
[SwitchB-pim] static-rp 10.13.1.4 bidir
```

4. Enable BIDIR-PIM.

```
[SwitchB-pim] bidir-pim enable
[SwitchB-pim] quit
```

5. Configure OSPF.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route direct
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure Switch C

1. Enable IP multicast routing.

```
<SwitchC> system-view
System View: return to User View with Ctrl+Z.
[SwitchC] multicast routing
[SwitchC-mrib] quit
```

2. Configure each interface and enable PIM-SM.

Create VLAN 33, and assign GigabitEthernet 1/0/4 to this VLAN.

```
[SwitchC] vlan 33
[SwitchC-vlan33] port gigabitethernet 1/0/4
[SwitchC-vlan33] quit
```

Assign an IP address to VLAN-interface 33, enable PIM-SM on the interface.

```
[SwitchC] interface vlan-interface 33
[SwitchC-Vlan-interface33] ip address 10.33.1.3 24
[SwitchC-Vlan-interface33] pim sm
[SwitchC-Vlan-interface33] quit
```

Create VLAN 13, and assign GigabitEthernet 1/0/3 to this VLAN.

```
[SwitchC] vlan 13
[SwitchC-vlan13] port gigabitethernet 1/0/3
[SwitchC-vlan13] quit
```

Assign an IP address to VLAN-interface 13, enable PIM-SM on the interface.

```
[SwitchC] interface vlan-interface 13
[SwitchC-Vlan-interface13] ip address 10.13.1.3 24
[SwitchC-Vlan-interface13] pim sm
[SwitchC-Vlan-interface13] quit
```

Create VLAN 23, and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchC] vlan 23
[SwitchC-vlan23] port gigabitethernet 1/0/2
[SwitchC-vlan23] quit
```

Assign an IP address to VLAN-interface 23, enable PIM-SM on the interface.

```
[SwitchC] interface vlan-interface 23
```

```
[SwitchC-Vlan-interface23] ip address 10.23.1.3 24
[SwitchC-Vlan-interface23] pim sm
[SwitchC-Vlan-interface23] quit
```

Create VLAN 102, and assign GigabitEthernet 1/0/1 to this VLAN.

```
[SwitchC] vlan 102
[SwitchC-vlan102] port gigabitethernet 1/0/1
[SwitchC-vlan102] quit
```

Assign an IP address to VLAN-interface 102, enable PIM-SM and IGMP on the interface.

```
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] ip address 10.102.1.1 24
[SwitchC-Vlan-interface102] igmp enable
[SwitchC-Vlan-interface102] quit
```

3. Specify the unused IP address 10.13.1.4 as a static RP.

```
[SwitchC] pim
[SwitchC-pim] static-rp 10.13.1.4 bidir
```

4. Enable BIDIR-PIM

```
[SwitchC-pim] bidir-pim enable
[SwitchC-pim] quit
```

5. Configure OSPF.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route direct
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Verifying the configuration

1. Verify that Switch A, Switch B, and Switch C have established PIM neighbor relationships.

Display PIM neighbor information on Switch A.

```
[SwitchA] display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface          Uptime   Expires  DR-Priority Mode
 10.12.1.2       Vlan12             00:02:27 00:01:45 1          B
 10.13.1.3       Vlan13             00:02:27 00:01:19 1          B
```

Display PIM neighbor information on Switch B.

```
[SwitchB] display pim neighbor
 Total Number of Neighbors = 2

 Neighbor        Interface          Uptime   Expires  DR-Priority Mode
 10.12.1.1       Vlan12             00:03:05 00:01:44 1          B
 10.23.1.3       Vlan23             00:13:49 00:01:29 1          B
```

Display PIM neighbor information on Switch C.

```
[SwitchC] display pim neighbor
 Total Number of Neighbors = 2
```

```
Neighbor       Interface         Uptime   Expires  DR-Priority Mode
10.13.1.1      Vlan13            00:03:28 00:01:39 1          B
10.23.1.2      Vlan23            00:14:05 00:01:36 1          B
```

2. Verify that VLAN-interface 12 on Switch A has been elected as the BSR on each switch.

Display BSR information on Switch A.

```
[SwitchA] display pim bsr-info
 Scope: non-scoped
    State: Elected
    Bootstrap timer: 00:01:18
    Elected BSR address: 10.12.1.1
      Priority: 64
      Hash mask length: 30
      Uptime: 00:04:01
    Candidate BSR address: 10.12.1.1
      Priority: 64
      Hash mask length: 30
```

Display BSR information on Switch B.

```
[SwitchB] display pim bsr-info
 Scope: non-scoped
    State: Accept Preferred
    Bootstrap timer: 00:00:26
    Elected BSR address: 10.12.1.1
      Priority: 64
      Hash mask length: 30
      Uptime: 00:10:41
```

Display BSR information on Switch C.

```
[SwitchC] display pim bsr-info
 Scope: non-scoped
    State: Accept Preferred
    Bootstrap timer: 00:02:08
    Elected BSR address: 10.12.1.1
      Priority: 64
      Hash mask length: 30
      Uptime: 00:15:41
```

3. Verify that VLAN-interface 12 on Switch A has been elected as the RP, and verify that the IP address of the static RP is 10.13.1.4 on each switch.

Display RP information on Switch A.

```
[SwitchA] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address             Priority  HoldTime  Uptime    Expires
       10.12.1.1 (local)       192      150      00:06:01  00:02:58

 Static RP information:
       RP address             ACL   Mode    Preferred
       10.13.1.4              ----  bidir   No
```

Display RP information on Switch B.

```
[SwatchB] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address            Priority  HoldTime  Uptime    Expires
       10.12.1.1             192       150       00:06:33  00:02:26

 Static RP information:
       RP address            ACL   Mode    Preferred
       10.13.1.4             ----  bidir   No
```

Display RP information on Switch C.

```
[SwitchC] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4 [B]
       RP address            Priority  HoldTime  Uptime    Expires
       10.12.1.1             192       150       00:06:51  00:02:05

Static RP information:
       RP address            ACL   Mode    Preferred
       10.13.1.4             ----  bidir   No
```

4. Verify that the DFs have been elected for BIDIR-PIM on each switch.

Display information about DFs for BIDIR-PIM on Switch A.

```
[SwitchA] display pim df-info
RP address: 10.12.1.1
  Interface: Vlan-interface100
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:01:09
    DF address: 10.10.1.1 (local)
  Interface: Vlan-interface12
    State    : -         DF preference: -
    DF metric : -         DF uptime    : -
    DF address: -
  Interface: Vlan-interface13
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:01:10
    DF address: 10.13.1.1 (local)

RP address: 10.13.1.4
  Interface: Vlan-interface100
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:00:07
    DF address: 10.10.1.1 (local)
  Interface: Vlan-interface12
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:00:07
    DF address: 10.12.1.1 (local)
  Interface: Vlan-interface13
```

```
    State    : -         DF preference: -
    DF metric : -         DF uptime    : -
    DF address: -
```

Display information about DFs for BIDIR-PIM on Switch B.

```
[SwatchB] display pim df-info
RP address: 10.12.1.1
  Interface: Vlan-interface12
    State    : -         DF preference: -
    DF metric : -         DF uptime    : -
    DF address: -
  Interface: Vlan-interface23
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:01:46
    DF address: 10.23.1.2 (local)
  Interface: Vlan-interface101
    State    : Win       DF preference: 0
    DF metric : 0         DF uptime    : 00:01:45
    DF address: 10.101.1.1 (local)

RP address: 10.13.1.4
  Interface: Vlan-interface12
    State    : Lose      DF preference: 0
    DF metric : 0         DF uptime    : 00:00:44
    DF address: 10.12.1.1
  Interface: Vlan-interface23
    State    : Lose      DF preference: 0
    DF metric : 0         DF uptime    : 00:00:53
    DF address: 10.23.1.3
  Interface: Vlan-interface101
    State    : Win       DF preference: 10
    DF metric : 2         DF uptime    : 00:00:53
    DF address: 10.101.1.1 (local)
```

Display information about DFs for BIDIR-PIM on Switch C.

```
[SwitchC] display pim df-info
RP address: 10.12.1.1
  Interface: Vlan-interface102
    State    : Win       DF preference: 10
    DF metric : 2         DF uptime    : 00:02:07
    DF address: 10.102.1.1 (local)
  Interface: Vlan-interface33
    State    : Win       DF preference: 10
    DF metric : 2         DF uptime    : 00:02:06
    DF address: 10.33.1.3 (local)
  Interface: Vlan-interface13
    State    : Lose      DF preference: 0
    DF metric : 0         DF uptime    : 00:02:07
    DF address: 10.13.1.1
  Interface: Vlan-interface23
```

```
    State    : Lose      DF preference: 0
    DF metric : 0        DF uptime    : 00:02:07
    DF address: 10.23.1.2

RP address: 10.13.1.4
  Interface: Vlan-interface102
    State    : Win       DF preference: 0
    DF metric : 0        DF uptime    : 00:01:24
    DF address: 10.102.1.1 (local)
  Interface: Vlan-interface33
    State    : Win       DF preference: 0
    DF metric : 0        DF uptime    : 00:01:23
    DF address: 10.33.1.3 (local)
  Interface: Vlan-interface13
    State    : -         DF preference: -
    DF metric : -        DF uptime    : -
    DF address: -
  Interface: Vlan-interface23
    State    : Win       DF preference: 0
    DF metric : 0        DF uptime    : 00:01:24
```

5. Verify that DFs for multicast forwarding are correct on each switch.

Display information about DFs for multicast forwarding on Switch A.

```
[SwitchA] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
    Flags: 0x0
    Uptime: 00:02:42
    RPF interface: Vlan-interface12
    List of 2 DF interfaces:
      1: Vlan-interface100
      2: Vlan-interface13

00002. RP address: 10.13.1.4
    Flags: 0x0
    Uptime: 00:01:41
    RPF interface: Vlan-interface13
    List of 2 DF interfaces:
      1: Vlan-interface100
      2: Vlan-interface12
```

Display information about DFs for multicast forwarding on Switch B.

```
[SwitchB] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
    Flags: 0x0
    Uptime: 00:03:18
    RPF interface: Vlan-interface12
```

```
    List of 2 DF interfaces:
      1: Vlan-interface23
      2: Vlan-interface101

00002. RP address: 10.13.1.4
    Flags: 0x0
    Uptime: 00:02:24
    RPF interface: Vlan-interface23
    List of 1 DF interfaces:
      1: Vlan-interface101
```

Display information about DFs for multicast forwarding on Switch C.

```
[SwitchC] display multicast forwarding df-info
Total 2 RPs, 2 matched

00001. RP address: 10.12.1.1
    Flags: 0x0
    Uptime: 00:03:38
    RPF interface: Vlan-interface23
    List of 2 DF interfaces:
      1: Vlan-interface102
      2: Vlan-interface33

00002. RP address: 10.13.1.4
    Flags: 0x0
    Uptime: 00:02:41
    RPF interface: Vlan-interface13
    List of 3 DF interfaces:
      1: Vlan-interface33
      2: Vlan-interface23
      3: Vlan-interface102
```

6. Send IGMP reports from Host A and Host B to join multicast group 225.1.1.1, and send multicast data from Source 1 and Source 2 to the group. (Details not shown.)

7. Verify that PIM forwarding entries have been correctly established on each switch.

Display information about PIM routing entries on Switch A.

```
[SwitchA] display pim routing-table
 Total 1 (*, G) entries; 0 (S, G) entries

 (*, 225.1.1.1)
    RP: 10.12.1.1 (local)
    Protocol: pim-bidir, Flag: WC LOC ACT
    UpTime: 00:21:59
    Upstream interface: Vlan-interface12
       Upstream neighbor: NULL
       RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
       1: Vlan-interface12
           Protocol: pim-bidir, UpTime: 00:21:59, Expires: -
```

```
        2: Vlan-interface13
            Protocol: pim-bidir, UpTime: 00:03:26, Expires: -
```

Display information about PIM routing entries on Switch B.

```
[SwitchB] display pim routing-table
 Total 1 (*, G) entries; 0 (S, G) entries

 (*, 225.1.1.1)
    RP: 10.12.1.1
    Protocol: pim-bidir, Flag: WC LOC ACT
    UpTime: 00:23:47
    Upstream interface: Vlan-interface12
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 3
        1: Vlan-interface12
            Protocol: pim-bidir, UpTime: 00:23:47, Expires: -
        2: Vlan-interface23
            Protocol: pim-bidir, UpTime: 00:21:56, Expires: -
        3: Vlan-interface101
            Protocol: igmp, UpTime: 00:23:47, Expires: -
```

Display information about PIM routing entries on Switch C.

```
[SwitchC] display pim routing-table
 Total 1 (*, G) entries; 0 (S, G) entries

 (*, 225.1.1.1)
    RP: 10.12.1.1
    Protocol: pim-bidir, Flag: WC ACT
    UpTime: 00:01:45
    Upstream interface: Vlan-interface23
        Upstream neighbor: 10.23.1.2
        RPF prime neighbor: 10.23.1.2
    Downstream interface(s) information:
    Total number of downstreams: 2
        1: Vlan-interface102
            Protocol: igmp, UpTime: 00:01:05, Expires: -
        2: Vlan-interface23
            Protocol: pim-bidir, UpTime: 00:00:53, Expires: -
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

- Switch A:

```
#
ospf 1
```

```
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
vlan 12 to 13
#
vlan 100
#
interface Vlan-interface12
 ip address 10.12.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface13
 ip address 10.13.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface100
 ip address 10.10.1.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
multicast routing
#
pim
 bidir-pim enable
 c-bsr 10.12.1.1
 c-rp 10.12.1.1 bidir
 static-rp 10.13.1.4 bidir
#
```

- Switch B:

```
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
vlan 12
#
Vlan 23
```

```
#
vlan 101
#
interface Vlan-interface12
 ip address 10.12.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface23
 ip address 10.23.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface101
 ip address 10.101.1.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 23
#
multicast routing
#
pim
 bidir-pim enable
 static-rp 10.13.1.4 bidir
#
```

- Switch C:

```
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
vlan 13
#
vlan 23
#
vlan 33
#
vlan 102
#
interface Vlan-interface13
```

```
 ip address 10.13.1.3 255.255.255.0
 pim sm
#
interface Vlan-interface23
 ip address 10.23.1.3 255.255.255.0
 pim sm
#
interface Vlan-interface33
 ip address 10.33.1.3 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 10.102.1.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 102
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 23
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 33
#
multicast routing
#
pim
 bidir-pim enable
 static-rp 10.13.1.4 bidir
#
```

Contents

Introduction

This document provides examples for configuring congestion avoidance and queue scheduling profiles.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of congestion avoidance and queue scheduling profiles.

Example: Configuring congestion avoidance and queue scheduling

Network configuration

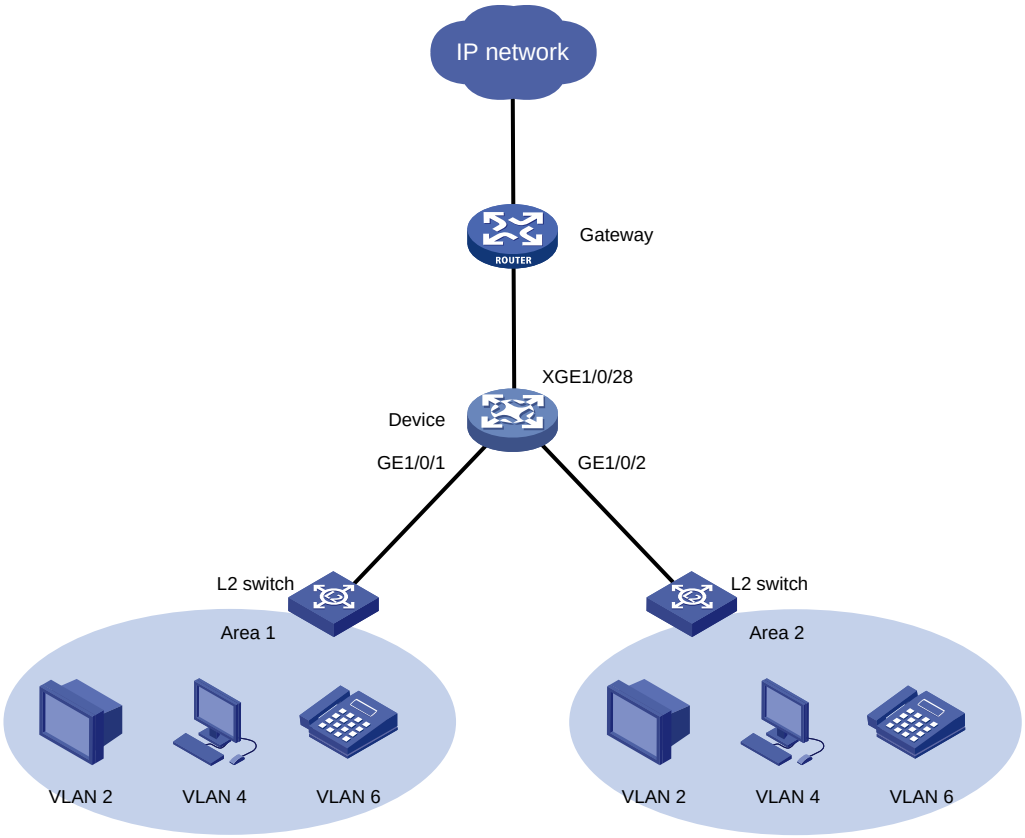
As shown in Figure 1, three types of traffic come from the Internet to the device through the gateway.

- **Voice traffic**—Transmitted in VLAN 6 and carries 802.1p priority 6.
- **Video traffic**—Transmitted in VLAN 4 and carries 802.1p priority 4.
- **Data traffic**—Transmitted in VLAN 2 and carries 802.1p priority 2.

Configure congestion avoidance and queue scheduling on the device to meet the following requirements:

- The voice traffic, video traffic, and data traffic are scheduled in the ratio of 1:2:2 when congestion occurs.
- WRED drop is used when serious congestion occurs.

Figure 1 Network diagram



Analysis

To configure congestion avoidance and queue scheduling, you must perform the following tasks:

- To assign different types of traffic to different queues, configure the inbound interface to trust the 802.1p priority in packets.
- To schedule the three types of traffic in the ratio of 1:2:2, assign their queues to one WRR group and configure weights for these queues.
- To minimize performance degradation for different types of traffic, use the drop parameters in Table 1.

Table 1 Drop parameters

Traffic type	Packet color	Lower limit	Upper limit	Drop probability
Voice	Yellow	1000	1500	3%
	Red	500	1000	30%
Video	Yellow	1000	1500	2%
	Red	500	1000	20%
Data	Yellow	1000	1500	1%
	Red	500	1000	10%

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI series	Release 6008 and later, Release 8106Pxx
S6525XE-HI series	Release 6008 and later, Release 8106Pxx
S5850 series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Release 11xx

S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C E152C E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

1. Allow VLANs for different types of traffic to pass through:

Create three VLANs .

```
<Device> system-view
```

```
[Device] vlan 2
[Device-vlan2] quit
[Device] vlan 4
[Device-vlan4] quit
[Device] vlan 6
[Device-vlan6] quit
```

Assign interfaces to VLANs.

```
[Device] interface ten-gigabitethernet 1/0/28
[Device-Ten-Gigabitethernet1/0/28] port link-type trunk
[Device-Ten-Gigabitethernet1/0/28] port trunk permit vlan 2 4 6
[Device-Ten-Gigabitethernet1/0/28] quit
[Device] interface gigabitethernet 1/0/1
[Device-Gigabitethernet1/0/1] port link-type trunk
[Device-Gigabitethernet1/0/1] port trunk permit vlan 2 4 6
[Device-Gigabitethernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-Gigabitethernet1/0/2] port link-type trunk
[Device-Gigabitethernet1/0/2] port trunk permit vlan 2 4 6
[Device-Gigabitethernet1/0/2] quit
```

2. Configure interface Gigabitethernet 1/0/28 to trust the 802.1p priority in packets.

```
[Device] interface ten-gigabitethernet 1/0/28
[Device-Ten-Gigabitethernet1/0/28] qos trust dot1p
[Device-Ten-Gigabitethernet1/0/28] quit
```

3. Configure WRR on Gigabitethernet 1/0//1 and Gigabitethernet 1/0//2:

Display the 802.1p-to-local precedence map to determine the local precedence for each type of traffic.

```
[Device] display qos map-table inbound dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

Enable weight-based WRR on Gigabitethernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-Gigabitethernet1/0/1] qos wrr weight
```

Configure the weights of queue 1 (for data traffic), queue 4 (for video traffic), and queue 6 (for voice traffic) as 2, 2, and 1, respectively.

```
[Device-Gigabitethernet1/0/1] qos wrr 1 group 1 weight 2
[Device-Gigabitethernet1/0/1] qos wrr 4 group 1 weight 2
[Device-Gigabitethernet1/0/1] qos wrr 6 group 1 weight 1
[Device-Gigabitethernet1/0/1] quit
```

Enable weight-based WRR on Gigabitethernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] qos wrr weight
```

Configure the weights of queue 1 (for data traffic), queue 4 (for video traffic), and queue 6 (for voice traffic) as 2, 2, and 1, respectively.

```
[Device-GigabitEthernet1/0/2] qos wrr 1 group 1 weight 2
[Device-GigabitEthernet1/0/2] qos wrr 4 group 1 weight 2
[Device-GigabitEthernet1/0/2] qos wrr 6 group 1 weight 1
[Device-GigabitEthernet1/0/2] quit
```

4. Configure congestion avoidance:

Configure a WRED table.

```
[Device] qos wred queue table droppolicy
[Device-wred-table-droppolicy] queue 6 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 3
[Device-wred-table-droppolicy] queue 6 drop-level 2 low-limit 500 high-limit 1000 discard-probability 30
[Device-wred-table-droppolicy] queue 4 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 2
[Device-wred-table-droppolicy] queue 4 drop-level 2 low-limit 500 high-limit 1000 discard-probability 20
[Device-wred-table-droppolicy] queue 1 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 1
[Device-wred-table-droppolicy] queue 1 drop-level 2 low-limit 500 high-limit 1000 discard-probability 10
[Device-wred-table-droppolicy] quit
```

Apply the WRED table to interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos wred apply droppolicy
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos wred apply droppolicy
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify the WRR configuration on interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[Device] display qos queue wrr interface
Interface: GigabitEthernet1/0/1
 Output queue: Weighted Round Robin queuing
 Queue ID     Queue name     Group     Weight
 ----------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         2
 5            ef             1         9
 6            cs6            1         1
 7            cs7            1         15
Interface: GigabitEthernet1/0/2
 Output queue: Weighted Round Robin queuing
```

```
 Queue ID     Queue name     Group     Weight
 -------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         4
 4            af4            1         2
 5            ef             1         9
 6            cs6            1         1
 7            cs7            1         15
```

Display the WRED table configuration.

```
Table name: droppolicy
Table type: Queue based WRED
QID   gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent  ECN
-------------------------------------------------------------------------------
0     100   1000  10     100   1000  10     100   1000  10     9         N
1     100   1000  10     1000  1500  1      500   1000  10     9         N
2     100   1000  10     100   1000  10     100   1000  10     9         N
3     100   1000  10     100   1000  10     100   1000  10     9         N
4     100   1000  10     1000  1500  2      500   1000  20     9         N
5     100   1000  10     100   1000  10     100   1000  10     9         N
6     100   1000  10     1000  1500  3      500   1000  30     9         N
7     100   1000  10     100   1000  10     100   1000  10     9         N
```

Configuration files

```
#
vlan 1
#
vlan 2
#
vlan 4
#
vlan 6
#
qos wred queue table droppolicy
 queue 1 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 1
 queue 1 drop-level 2 low-limit 500 high-limit 1000 discard-probability 10
 queue 4 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 2
 queue 4 drop-level 2 low-limit 500 high-limit 1000 discard-probability 20
 queue 6 drop-level 1 low-limit 1000 high-limit 1500 discard-probability 3
 queue 6 drop-level 2 low-limit 500 high-limit 1000 discard-probability 30
#
interface Gigabitethernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 4 6
 qos wrr weight
```

```
 qos wrr af1 group 1 weight 2
 qos wrr af4 group 1 weight 2
 qos wrr cs6 group 1 weight 1
 qos wred apply droppolicy
#
interface Gigabitethernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 4 6
 qos wrr weight
 qos wrr af1 group 1 weight 2
 qos wrr af4 group 1 weight 2
 qos wrr cs6 group 1 weight 1
 qos wred apply droppolicy
#
interface Ten-Gigabitethernet1/0/28
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 4 6
#
return
```

Contents

Introduction

This document provides static LSP and LDP LSP configuration examples.

The following table shows the differences between a static LSP and an LDP LSP:

LSP type	Establishment	Feature	Application scenario
Static LSP	You establish a static LSP by specifying the incoming and outgoing labels on ingress, transit, and egress nodes of the forwarding path.	• Consumes fewer resources. • Cannot automatically adapt to network topology changes.	Small and stable networks with simple topologies.
LDP LSP	You establish an LDP LSP by configuring MPLS LDP. LDP classifies FECs, distributes FEC-label mappings, and establishes and maintains LSPs.	• Consumes more resources. • Automatically adapts to network topology changes.	Large and unstable networks with complicated topologies.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

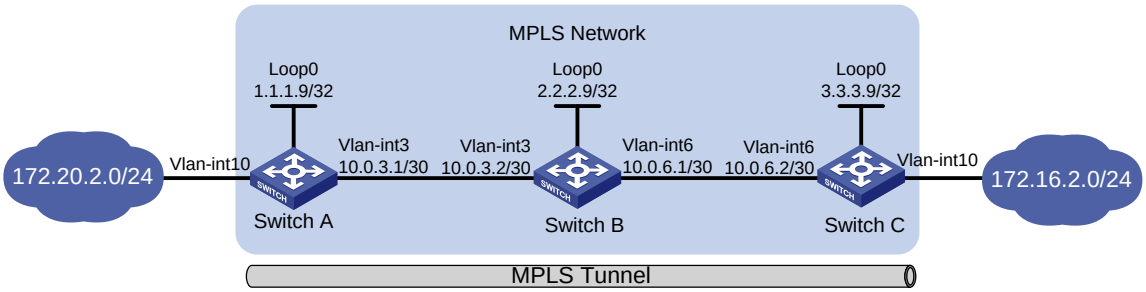
This document assumes that you have basic knowledge of MPLS and LDP.

Example: Configuring static LSPs

Network configuration

As shown in Figure 1, establish static LSPs between Switch A and Switch C to allow communication between subnets 172.20.2.0/24 and 172.16.2.0/24 over the MPLS network.

Figure 1 Network diagram



Analysis

LSPs are unidirectional. To ensure that data can be bidirectionally forwarded, configure an LSP for each direction of the data forwarding path, and specify the ingress, transit, and egress nodes for each LSP.

To direct traffic to an LSP for MPLS forwarding, make sure the ingress node has a route to the FEC destination of the LSP. This example uses a static route. Route configuration is not needed on the transit and egress nodes.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx switch series, Release 6628Pxx switch series
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx switch series
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx switch series
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5560X-HI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5500V2-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30F switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S6520X-SI switch series S6520-SI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5000-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4600 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
ES5500 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5560S-EI switch series S5560S-SI switch series	Not supported

Hardware	Software version
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series	Not supported

Hardware	Software version
WS5810-WiNet switch series	
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure a static LSP, follow these restrictions and guidelines:

- Make sure the outgoing label specified on an LSR is the same as the incoming label specified on the directly connected downstream LSR.
- If you configure a static IP route for the LSP, specify the same next hop or outgoing interface for the static route and the static LSP.
- On the ingress or transit node of the static LSP, do not specify the public address of a local interface as the next hop address of the static LSP.
- MPLS adds a label or multiple labels to packets. After MPLS is enabled on a VLAN interface, configure jumboframe support on the ports in the VLAN to avoid MPLS packet dropping when the packet size exceeds the interface MTU.

Procedures

1. Configure IP addresses and masks for interfaces, including the loopback interfaces, as shown in Figure 1. (Details not shown.)
2. Configure a static route to the destination address of each LSP:

   # Configure a static route to the FEC destination of the LSP from Switch A to Switch C.

   ```
   <SwitchA> system-view
   [SwitchA] ip route-static 172.16.2.1 24 10.0.3.2
   ```

   # Configure a static route to the FEC destination of the LSP from Switch C to Switch A.

   ```
   <SwitchC> system-view
   [SwitchC] ip route-static 172.20.2.1 24 10.0.6.1
   ```

   # Verify that the static route has been created on the ingress nodes, for example, on Switch A.

   ```
   [SwitchA] display ip routing-table

   Destinations : 13        Routes : 13

   Destination/Mask    Proto  Pre  Cost         NextHop         Interface
   0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
   172.16.2.1/24       Static 60   0           10.0.3.2        Vlan3
   10.0.3.0/24         Direct 0    0           10.0.3.1        Vlan3
   10.0.3.0/32         Direct 0    0           10.0.3.1        Vlan3
   10.0.3.1/32         Direct 0    0           127.0.0.1       InLoop0
   1.1.1.9/32          Direct 0    0           127.0.0.1       InLoop0
   ```

```
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

3. Configure basic MPLS on the switches:

Configure Switch A.

```
[SwitchA] mpls lsr-id 1.1.1.9
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] mpls enable
[SwitchA-Vlan-interface3] quit
```

Configure Switch B.

```
[SwitchB] mpls lsr-id 2.2.2.9
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] mpls enable
[SwitchB-Vlan-interface3] quit
[SwitchB] interface vlan-interface 6
[SwitchB-Vlan-interface6] mpls enable
[SwitchB-Vlan-interface6] quit
```

Configure Switch C.

```
[SwitchC] mpls lsr-id 3.3.3.9
[SwitchC] interface vlan-interface 6
[SwitchC-Vlan-interface6] mpls enable
[SwitchC-Vlan-interface6] quit
```

4. Configure a static LSP from Switch A to Switch C:

Configure the ingress node Switch A. Specify the LSP name as **AtoC**, destination address as **172.16.2.1/24**, next hop as **10.0.3.2**, and outgoing label as **30**.

```
[SwitchA] static-lsp ingress AtoC destination 172.16.2.1 24 nexthop 10.0.3.2
out-label 30
```

Configure the transit node Switch B. Specify the LSP name as **AtoC**, incoming label as **30**, next hop as **10.0.6.2**, and outgoing label as **50**.

```
[SwitchB] static-lsp transit AtoC in-label 30 nexthop 10.0.6.2 out-label 50
```

Configure the egress node Switch C. Specify the LSP name as **AtoC** and incoming label as **50**.

```
[SwitchC] static-lsp egress AtoC in-label 50
```

5. Configure a static LSP from Switch C to Switch A:

Configure the ingress node Switch C. Specify the LSP name as **CtoA**, destination address as **172.20.2.1/24**, next hop as **10.0.6.1**, and outgoing label as **40**.

```
[SwitchC] static-lsp ingress CtoA destination 172.20.2.1 24 nexthop 10.0.6.1
out-label 40
```

Configure the transit node Switch B. Specify the LSP name as **CtoA**, incoming label as **40**, next hop as **10.0.3.1**, and outgoing label as **70**.

```
[SwitchB] static-lsp transit CtoA in-label 40 nexthop 10.0.3.1 out-label 70
```

Configure the egress node Switch A. Specify the LSP name as **CtoA** and incoming label as **70**.

```
[SwitchA] static-lsp egress CtoA in-label 70
```

Verifying the configuration

Display static LSP information on switches, for example, on Switch A.

```
[SwitchA] display mpls static-lsp
Total: 2
Name            FEC                In/Out Label Nexthop/Out Interface    State
AtoC            172.16.2.1/24      NULL/30      10.0.3.2                 Up
CtoA            -/-                70/NULL      -                        Up
```

Test the connectivity of the LSP from Switch A to Switch C.

```
[SwitchA] ping mpls -a 172.20.2.1 ipv4 172.16.2.0 24
MPLS ping FEC 172.16.2.0/24 with 100 bytes of data:
100 bytes from 10.0.6.2: Sequence=1 time=3 ms
100 bytes from 10.0.6.2: Sequence=2 time=2 ms
100 bytes from 10.0.6.2: Sequence=3 time=2 ms
100 bytes from 10.0.6.2: Sequence=4 time=2 ms
100 bytes from 10.0.6.2: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.16.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

Test the connectivity of the LSP from Switch C to Switch A.

```
[SwitchC] ping mpls -a 172.16.2.1 ipv4 172.20.2.0 24
MPLS ping FEC 172.20.2.0/24 with 100 bytes of data:
100 bytes from 10.0.3.2: Sequence=1 time=3 ms
100 bytes from 10.0.3.2: Sequence=2 time=2 ms
100 bytes from 10.0.3.2: Sequence=3 time=2 ms
100 bytes from 10.0.3.2: Sequence=4 time=2 ms
100 bytes from 10.0.3.2: Sequence=5 time=27 ms

--- Ping statistics for FEC 172.20.2.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/7/27 ms
```

Configuration files

- Switch A:

```
#
 mpls lsr-id 1.1.1.9
#
vlan 3
#
vlan 10
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface3
```

```
 ip address 10.0.3.1 255.255.255.0
 mpls enable
#
interface Vlan-interface10
 ip address 172.20.2.1 255.255.255.0
#
 ip route-static 172.16.2.1 255.255.255.0 10.0.3.2
#
 static-lsp ingress AtoC destination 172.16.2.1 24 nexthop 10.0.3.2 out-label 30
 static-lsp egress CtoA in-label 70
#
```

- Switch B:

```
#
 mpls lsr-id 2.2.2.9
#
vlan 3
#
vlan 6
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.0.3.2 255.255.255.0
 mpls enable
#
interface Vlan-interface6
 ip address 10.0.6.1 255.255.255.0
 mpls enable
#
 static-lsp transit AtoC in-label 30 nexthop 10.0.6.2 out-label 50
 static-lsp transit CtoA in-label 40 nexthop 10.0.3.1 out-label 70
#
```

- Switch C:

```
#
 mpls lsr-id 3.3.3.9
#
vlan 6
#
vlan 10
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface6
 ip address 10.0.6.2 255.255.255.0
 mpls enable
#
```

```
interface Vlan-interface10
 ip address 172.16.2.1 255.255.255.0
#
 ip route-static 172.20.2.1 255.255.255.0 10.0.6.2
#
 static-lsp ingress CtoA destination 172.20.2.1 24 nexthop 10.0.6.1 out-label 40
 static-lsp egress AtoC in-label 50
#
```

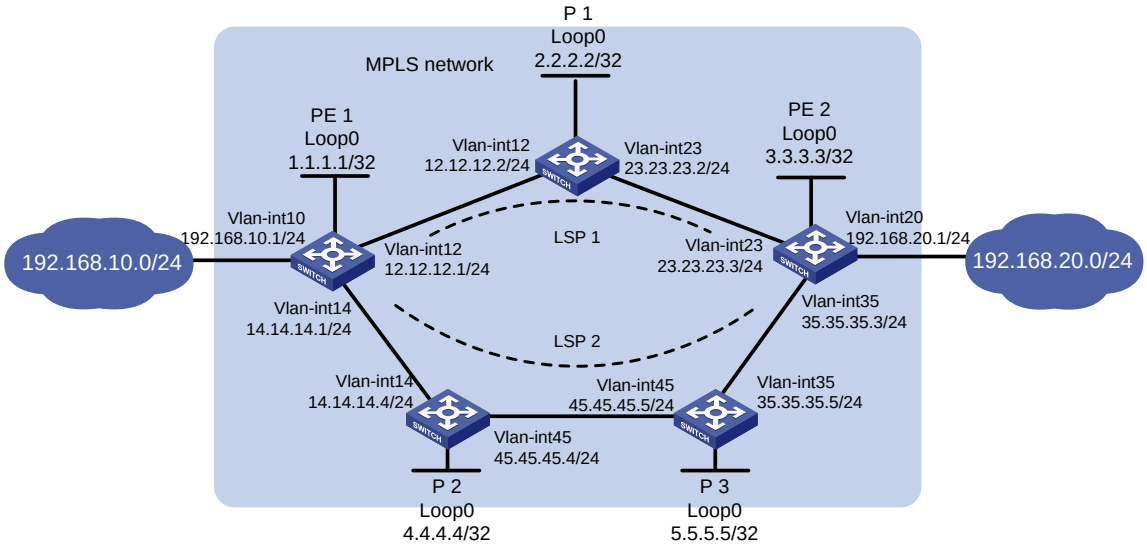
Example: Configuring LDP LSPs

Network configuration

As shown in Figure 2, two paths are available for PE 1 and PE 2 to communicate with each other.

- Configure LDP to establish LSPs between PE 1 and PE 2 to allow communication between subnets 192.168.10.0/24 and 192.168.20.0/24 over the MPLS network.
  - Use LSP 1 as the primary path.
  - Use LSP 2 as the backup path, which takes over LSP 1 when LSP 1 fails.
- Configure LDP to establish LSPs only for destinations 1.1.1.1/32, 2.2.2.2/32, 3.3.3.3/32, 4.4.4.4/32, 5.5.5.5/32, 192.168.10.0/24, and 192.168.20.0/24.

Figure 2 Network diagram



Analysis

To establish LDP LSPs, configure a routing protocol to ensure IP connectivity among the devices. This example uses OSPF.

To use LSP 1 as the primary path and LSP 2 as the backup, configure the routes for LSP 1 and LSP 2 as the primary and backup routes, respectively. This example uses OSPF. The OSPF cost of the route for LSP 1 is smaller than that for LSP 2. Therefore, LSP 1 is used when it is available.

To control LSP establishment, configure LSP generation policies on each LSR.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx switch series, Release 6628Pxx switch series
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx switch series
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx switch series
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5560X-HI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5500V2-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30F switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S6520X-SI switch series S6520-SI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5000-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4600 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
ES5500 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series	Not supported

Hardware	Software version
S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Before configuring LDP LSPs, make sure STP is disabled or each VLAN has been mapped to an MSTP instance.

1. Configure IP addresses and masks for interfaces, including the loopback interfaces, as shown in Figure 2. (Details not shown.)
2. Configure OSPF on each switch to ensure IP connectivity:

   # Configure PE 1.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

   # Configure P 1.

```
[P1] ospf
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

   # Configure P 2.

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

   # Configure P 3.

```
[P3] ospf
[P3-ospf-1] area 0
[P3-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[P3-ospf-1-area-0.0.0.0] network 45.45.45.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
[P3-ospf-1-area-0.0.0.0] quit
[P3-ospf-1] quit
```

   # Configure PE 2.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 35.35.35.0 0.0.0.255
```

```
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

On each switch, for example, on PE 1, verify that the switches have learned the routes to each other.

```
[PE1] display ospf routing

          OSPF Process 1 with Router ID 1.1.1.1
                    Routing Table
                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 45.45.45.0/24      2        Transit 14.14.14.4      5.5.5.5         0.0.0.0
 35.35.35.0/24      3        Transit 14.14.14.4      5.5.5.5         0.0.0.0
 35.35.35.0/24      3        Transit 12.12.12.2      5.5.5.5         0.0.0.0
 192.168.10.0/24    1        Stub    192.168.10.1    1.1.1.1         0.0.0.0
 5.5.5.5/32         2        Stub    14.14.14.4      5.5.5.5         0.0.0.0
 14.14.14.0/24      1        Transit 14.14.14.1      4.4.4.4         0.0.0.0
 23.23.23.0/24      2        Transit 12.12.12.2      3.3.3.3         0.0.0.0
 4.4.4.4/32         1        Stub    14.14.14.4      4.4.4.4         0.0.0.0
 3.3.3.3/32         2        Stub    12.12.12.2      3.3.3.3         0.0.0.0
 12.12.12.0/24      1        Transit 12.12.12.1      2.2.2.2         0.0.0.0
 2.2.2.2/32         1        Stub    12.12.12.2      2.2.2.2         0.0.0.0
 1.1.1.1/32         0        Stub    1.1.1.1         1.1.1.1         0.0.0.0
 192.168.20.0/24    3        Stub    12.12.12.2      3.3.3.3         0.0.0.0
```

On each switch, for example, on PE 1, verify that OSPF neighbor relationships in Full state have been established between PE 1, P devices, and PE 2.

```
[PE1] display ospf peer verbose
          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors

 Area 0.0.0.0 interface 14.14.14.1(Vlan-interface14)'s neighbors
 Router ID: 4.4.4.4          Address: 14.14.14.4       GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 14.14.14.4  BDR: 14.14.14.1  MTU: 0
   Options is 0x42 (-|O|-|-|-|-|E|-)
   Dead timer due in 40  sec
   Neighbor is up for 00:03:30
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled

                  Neighbors

 Area 0.0.0.0 interface 12.12.12.1(Vlan-interface12)'s neighbors
 Router ID: 2.2.2.2          Address: 12.12.12.2       GR state: Normal
   State: Full  Mode: Nbr is master  Priority: 1
   DR: 12.12.12.2  BDR: 12.12.12.1  MTU: 0
```

```
  Options is 0x42 (-|O|-|-|-|-|E|-)
  Dead timer due in 36  sec
  Neighbor is up for 00:03:24
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 6
  BFD status: Disabled

Last Neighbor Down Event:
Router ID: 4.4.4.4
Local Address: 14.14.14.1
Remote Address: 14.14.14.4
Time: May 14 09:07:19 2014
Reason: Reset ospf command was performed
```

3. Configure basic MPLS and MPLS LDP:

Configure PE 1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
[PE1] interface vlan-interface 14
[PE1-Vlan-interface14] mpls enable
[PE1-Vlan-interface14] mpls ldp enable
[PE1-Vlan-interface14] quit
```

Configure P 1.

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
[P1-ldp] quit
[P1] interface vlan-interface 12
[P1-Vlan-interface12] mpls enable
[P1-Vlan-interface12] mpls ldp enable
[P1-Vlan-interface12] quit
[P1] interface vlan-interface 23
[P1-Vlan-interface23] mpls enable
[P1-Vlan-interface23] mpls ldp enable
[P1-Vlan-interface23] quit
```

Configure P 2.

```
[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface vlan-interface 14
[P2-Vlan-interface14] mpls enable
[P2-Vlan-interface14] mpls ldp enable
[P2-Vlan-interface14] quit
[P2] interface vlan-interface 45
[P2-Vlan-interface45] mpls enable
```

```
[P2-Vlan-interface45] mpls ldp enable
[P2-Vlan-interface45] quit
```

Configure P 3.

```
[P3] mpls lsr-id 5.5.5.5
[P3] mpls ldp
[P3-ldp] quit
[P3] interface vlan-interface 45
[P3-Vlan-interface45] mpls enable
[P3-Vlan-interface45] mpls ldp enable
[P3-Vlan-interface45] quit
[P3] interface vlan-interface 35
[P3-Vlan-interface35] mpls enable
[P3-Vlan-interface35] mpls ldp enable
[P3-Vlan-interface35] quit
```

Configure PE 2.

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface vlan-interface 23
[PE2-Vlan-interface23] mpls enable
[PE2-Vlan-interface23] mpls ldp enable
[PE2-Vlan-interface23] quit
[PE2] interface vlan-interface 35
[PE2-Vlan-interface35] mpls enable
[PE2-Vlan-interface35] mpls ldp enable
[PE2-Vlan-interface35] quit
```

On each switch, for example, on PE 1, verify that LDP sessions in Operational state have been established between PE 1, P devices, and PE 2.

```
[PE1 display mpls ldp peer
Total number of peers: 2
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.2:0               Operational   Passive  Off  Off  55/55
4.4.4.4:0               Operational   Passive  Off  Off  6/6
```

4. Configure LSP generation policies:

On PE 1, create IP prefix list **PE1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE1] ip prefix-list PE1 index 10 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 20 permit 2.2.2.2 32
[PE1] ip prefix-list PE1 index 30 permit 3.3.3.3 32
[PE1] ip prefix-list PE1 index 40 permit 4.4.4.4 32
[PE1] ip prefix-list PE1 index 50 permit 5.5.5.5 32
[PE1] ip prefix-list PE1 index 60 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 70 permit 192.168.20.0 24
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

On P 1, create IP prefix list **P1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P1] ip prefix-list P1 index 10 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 20 permit 2.2.2.2 32
[P1] ip prefix-list P1 index 30 permit 3.3.3.3 32
[P1] ip prefix-list P1 index 40 permit 4.4.4.4 32
[P1] ip prefix-list P1 index 50 permit 5.5.5.5 32
[P1] ip prefix-list P1 index 60 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 70 permit 192.168.20.0 24
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

On P 2, create IP prefix list **P2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P2] ip prefix-list P2 index 10 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 20 permit 2.2.2.2 32
[P2] ip prefix-list P2 index 30 permit 3.3.3.3 32
[P2] ip prefix-list P2 index 40 permit 4.4.4.4 32
[P2] ip prefix-list P2 index 50 permit 5.5.5.5 32
[P2] ip prefix-list P2 index 60 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 70 permit 192.168.20.0 24
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

On P 3, create IP prefix list **P3**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P3] ip prefix-list P3 index 10 permit 1.1.1.1 32
[P3] ip prefix-list P3 index 20 permit 2.2.2.2 32
[P3] ip prefix-list P3 index 30 permit 3.3.3.3 32
[P3] ip prefix-list P3 index 40 permit 4.4.4.4 32
[P3] ip prefix-list P3 index 50 permit 5.5.5.5 32
[P3] ip prefix-list P3 index 60 permit 192.168.10.0 24
[P3] ip prefix-list P3 index 70 permit 192.168.20.0 24
[P3] mpls ldp
[P3-ldp] lsp-trigger prefix-list P3
[P3-ldp] quit
```

On PE 2, create IP prefix list **PE2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE2] ip prefix-list PE2 index 10 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 20 permit 2.2.2.2 32
[PE2] ip prefix-list PE2 index 30 permit 3.3.3.3 32
[PE2] ip prefix-list PE2 index 40 permit 4.4.4.4 32
[PE2] ip prefix-list PE2 index 50 permit 5.5.5.5 32
[PE2] ip prefix-list PE2 index 60 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 70 permit 192.168.20.0 24
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

Verifying the configuration

Display LDP LSP information on PE 1. The output shows that the next hop is P 1 for the LSP associated with FEC 192.168.20.0/24.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup, N/A – unavailable
FECs: 7            Ingress: 5          Transit: 5      Egress: 2
FEC                In/Out Label        Nexthop         OutInterface/LSINDEX
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1151(L)
2.2.2.2/32         -/3                 12.12.12.2      Vlan12
                   1151/3              12.12.12.2      Vlan12
                   -/1150(L)
3.3.3.3/32         -/1150              12.12.12.2      Vlan12
                   1150/1150           12.12.12.2      Vlan12
                   -/1148(L)
4.4.4.4/32         -/1149(L)
                   -/3                 14.14.14.4      Vlan14
                   1149/3              14.14.14.4      Vlan14
5.5.5.5/32         -/1148(L)
                   -/1149              14.14.14.4      Vlan14
                   1148/1149           14.14.14.4      Vlan14
192.168.10.0/24    1147/-
192.168.20.0/24    -/1147              12.12.12.2      Vlan12
                   1146/1147           12.12.12.2      Vlan12
                   -/1147(L)
```

Power down P 1 and execute the **`display mpls ldp lsp`** command on PE 1. The output shows that the next hop becomes P 2 for the LSP associated with FEC 192.168.20.0/24.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup, N/A – unavailable
FECs: 7            Ingress: 5          Transit: 5      Egress: 2
FEC                In/Out Label        Nexthop         OutInterface/LSINDEX
1.1.1.1/32         3/-
                   -/1150(L)
2.2.2.2/32         -/1149              14.14.14.4      Vlan14
                   1150/1149           14.14.14.4      Vlan14
3.3.3.3/32         -/1148              14.14.14.4      Vlan14
                   1147/1148           14.14.14.4      Vlan14
4.4.4.4/32         -/3                 14.14.14.4      Vlan14
                   1149/3              14.14.14.4      Vlan14
5.5.5.5/32         -/1151              14.14.14.4      Vlan14
                   1148/1151           14.14.14.4      Vlan14
192.168.10.0/24    1151/-
                   -/1146(L)
192.168.20.0/24    -/1147              14.14.14.4      Vlan14
                   1146/1147           14.14.14.4      Vlan14
```

Use the following command on PE 1 to verify its connectivity to PE 2.

```
[PE1] ping mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS ping FEC 192.168.20.0/24 with 100 bytes of data:
100 bytes from 23.23.23.3: Sequence=1 time=2 ms
100 bytes from 23.23.23.3: Sequence=2 time=2 ms
100 bytes from 23.23.23.3: Sequence=3 time=2 ms
100 bytes from 23.23.23.3: Sequence=4 time=2 ms
100 bytes from 23.23.23.3: Sequence=5 time=2 ms

--- Ping statistics for FEC 192.168.20.0/24 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
Round-trip min/avg/max = 2/2/2 ms
```

Configuration files

- PE 1:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
vlan 10
#
vlan 12
#
vlan 14
#
mpls ldp
 lsp-trigger prefix-list PE1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface14
 ip address 14.14.14.1 255.255.255.0
 mpls enable
```

```
 mpls ldp enable
#
 ip prefix-list PE1 index 10 permit 1.1.1.1 32
 ip prefix-list PE1 index 20 permit 2.2.2.2 32
 ip prefix-list PE1 index 30 permit 3.3.3.3 32
 ip prefix-list PE1 index 40 permit 4.4.4.4 32
 ip prefix-list PE1 index 50 permit 5.5.5.5 32
 ip prefix-list PE1 index 60 permit 192.168.10.0 24
 ip prefix-list PE1 index 70 permit 192.168.20.0 24
#
```

- P 1:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
vlan 12
#
vlan 23
#
mpls ldp
 lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface23
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
#
 ip prefix-list P1 index 10 permit 1.1.1.1 32
 ip prefix-list P1 index 20 permit 2.2.2.2 32
 ip prefix-list P1 index 30 permit 3.3.3.3 32
 ip prefix-list P1 index 40 permit 4.4.4.4 32
 ip prefix-list P1 index 50 permit 5.5.5.5 32
 ip prefix-list P1 index 60 permit 192.168.10.0 24
 ip prefix-list P1 index 70 permit 192.168.20.0 24
```

```
#
```

- P 2:

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 45.45.45.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
vlan 14
#
vlan 45
#
mpls ldp
 lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface14
 ip address 14.14.14.4 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface45
 ip address 45.45.45.4 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 1.1.1.1 32
 ip prefix-list P1 index 20 permit 2.2.2.2 32
 ip prefix-list P1 index 30 permit 3.3.3.3 32
 ip prefix-list P1 index 40 permit 4.4.4.4 32
 ip prefix-list P1 index 50 permit 5.5.5.5 32
 ip prefix-list P1 index 60 permit 192.168.10.0 24
 ip prefix-list P1 index 70 permit 192.168.20.0 24
#
```

- P 3:

```
#
ospf 1
 area 0.0.0.0
  network 5.5.5.5 0.0.0.0
  network 35.35.35.0 0.0.0.255
  network 45.45.45.0 0.0.0.255
#
 mpls lsr-id 5.5.5.5
```

```
#
vlan 35
#
vlan 45
#
mpls ldp
 lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface35
 ip address 35.35.35.5 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface45
 ip address 45.45.45.5 255.255.255.0
 mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 1.1.1.1 32
 ip prefix-list P1 index 20 permit 2.2.2.2 32
 ip prefix-list P1 index 30 permit 3.3.3.3 32
 ip prefix-list P1 index 40 permit 4.4.4.4 32
 ip prefix-list P1 index 50 permit 5.5.5.5 32
 ip prefix-list P1 index 60 permit 192.168.10.0 24
 ip prefix-list P1 index 70 permit 192.168.20.0 24
#
```

- PE 2:

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 35.35.35.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
 mpls lsr-id 3.3.3.3
#
vlan 20
#
vlan 23
#
vlan 35
#
mpls ldp
 lsp-trigger prefix-list PE2
```

```
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface35
 ip address 5.35.35.3 255.255.255.0
mpls enable
 mpls ldp enable
#
 ip prefix-list P1 index 10 permit 1.1.1.1 32
 ip prefix-list P1 index 20 permit 2.2.2.2 32
 ip prefix-list P1 index 30 permit 3.3.3.3 32
 ip prefix-list P1 index 40 permit 4.4.4.4 32
 ip prefix-list P1 index 50 permit 5.5.5.5 32
 ip prefix-list P1 index 60 permit 192.168.10.0 24
 ip prefix-list P1 index 70 permit 192.168.20.0 24
#
```

Contents

Introduction

This document provides MPLS L3VPN configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

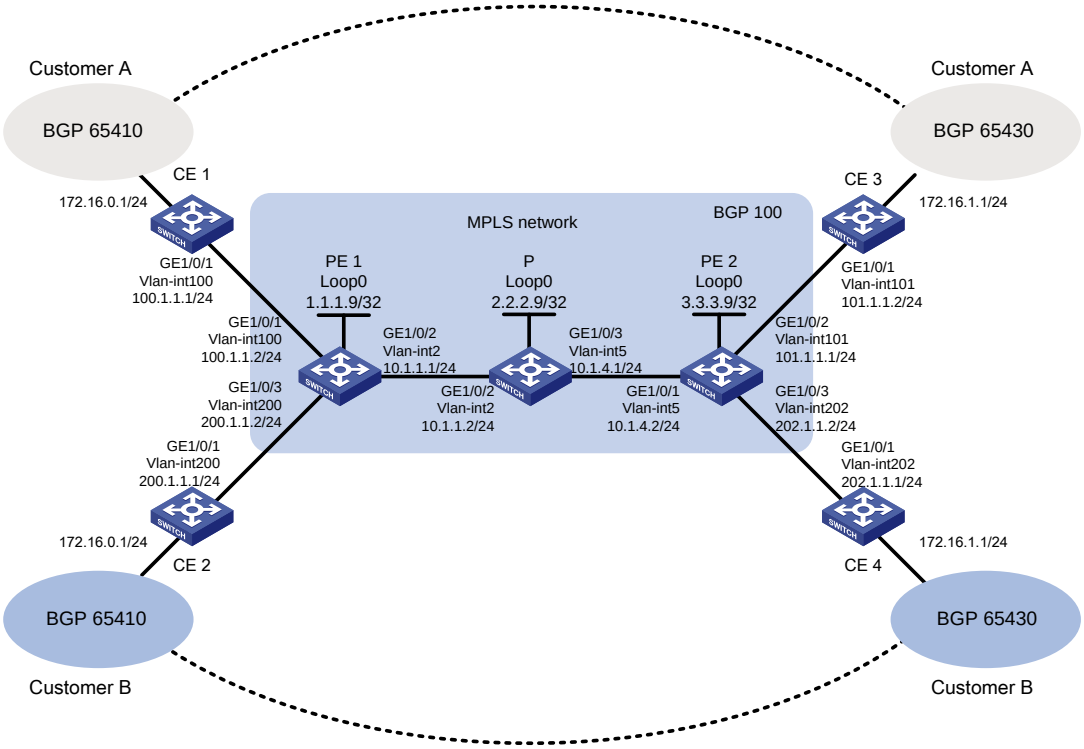
This document assumes that you have basic knowledge of MPLS L3VPN.

Example: Configuring MPLS L3VPN

Network configuration

As shown in Figure 1, configure MPLS L3VPN to allow communication between different sites of a customer and to isolate different customers.

Figure 1 Network diagram



Analysis

To generate inner labels, and deliver VPN routing information to the remote PE, configure MP-BGP peers between PEs.

To generate outer labels to tunnel the VPN packets over the MPLS backbone, configure a routing protocol and MPLS LDP on the MPLS backbone.

To identify routing information for different customers on PEs, perform the following tasks on each PE:

- Create a VPN instance for each customer.
- Configure an RD and route targets for each VPN instance.
- Redistribute internal routes of each site to the corresponding VPN instance.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported

Hardware	Software version
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported

Hardware	Software version
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Associating an interface with a VPN instance deletes the IP address of the interface. You must reconfigure the interface's IP address after the association.

Procedures

1. Configure OSPF on the MPLS backbone to ensure IP connectivity within the backbone:

On PE 1, configure IP addresses for the loopback interface and the core-facing interface.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] vlan 2
[PE1-vlan2] port gigabitethernet 1/0/2
[PE1-vlan2] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] quit
```

On PE 1, configure OSPF to advertise backbone networks.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

On P, configure IP addresses for interfaces, including the loopback interface.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] vlan 2
[P-vlan2] port gigabitethernet 1/0/2
[P-vlan2] quit
[P] vlan 5
[P-vlan5] port gigabitethernet 1/0/3
[P-vlan5] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
[P] interface vlan-interface 5
[P-Vlan-interface5] ip address 10.1.4.1 24
```

```
[P-Vlan-interface5] quit
```

On P, configure OSPF to advertise backbone networks.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

On PE 2, configure IP addresses for the loopback interface and the core-facing interface.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] vlan 5
[PE2-vlan5] port gigabitethernet 1/0/1
[PE2-vlan5] quit
[PE2] interface vlan-interface 5
[PE2-Vlan-interface5] ip address 10.1.4.2 24
[PE2-Vlan-interface5] quit
```

On PE 2, configure OSPF to advertise backbone networks.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Verify that OSPF neighbor relationships in Full state have been established on the backbone devices.

```
[PE1] display ospf peer verbose
          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors
 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface2)'s neighbors
 Router ID: 2.2.2.9          Address: 10.1.1.2        GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 10.1.1.2  BDR: 10.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 38  sec
   Neighbor is up for 17:30:25
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
```

Verify that the PEs have learned the routes to the loopback interfaces of each other.

```
[PE1] display ip routing-table protocol ospf
Summary Count : 5
OSPF Routing table Status : <Active>
Summary Count : 3
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
```

```
2.2.2.9/32          OSPF   10   1            10.1.1.2        Vlan2
3.3.3.9/32          OSPF   10   2            10.1.1.2        Vlan2
10.1.4.0/24         OSPF   10   2            10.1.1.2        Vlan2
OSPF Routing table Status : <Inactive>
Summary Count : 2
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.1.9/32          OSPF   10   0            1.1.1.9         Loop0
10.1.1.0/24         OSPF   10   1            10.1.1.1        Vlan2
```

2. Configure basic MPLS and MPLS LDP on the MPLS backbone to establish LDP LSPs:

Configure PE 1.

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] mpls enable
[PE1-Vlan-interface2] mpls ldp enable
[PE1-Vlan-interface2] quit
```

Configure P.

```
[P] mpls lsr-id 2.2.2.9
[P] mpls ldp
[P-ldp] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls enable
[P-Vlan-interface2] mpls ldp enable
[P-Vlan-interface2] quit
[P] interface vlan-interface 5
[P-Vlan-interface5] mpls enable
[P-Vlan-interface5] mpls ldp enable
[P-Vlan-interface5] quit
```

Configure PE 2.

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface vlan-interface 5
[PE2-Vlan-interface5] mpls enable
[PE2-Vlan-interface5] mpls ldp enable
[PE2-Vlan-interface5] quit
```

Verify that LDP sessions in Operational state have been established.

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  5/5
```

Verify that the LSPs have been established by LDP.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 4            Ingress: 1          Transit: 1      Egress: 3

FEC                In/Out Label        Nexthop         OutInterface
```

```
1.1.1.9/32        3/-
                  -/1151(L)
2.2.2.9/32        -/3               10.1.1.2        Vlan2
                  1151/3            10.1.1.2        Vlan2
3.3.3.9/32        -/1150            10.1.1.2        Vlan2
                  1150/1150         10.1.1.2        Vlan2
```

3. Configure VPN instances on PEs to allow CE access:

On PE 1, create VPN instance **customerA** for Customer A.

```
[PE1] ip vpn-instance customerA
```

On PE 1, configure the RD as 100:1 for the VPN instance.

```
[PE1-vpn-instance-customerA] route-distinguisher 100:1
```

On PE 1, specify the import target as 111:1 and the export target as 222:1 for the VPN instance. You can configure the same value for both the import and export targets to simplify management.

```
[PE1-vpn-instance-customerA] vpn-target 111:1 import-extcommunity
[PE1-vpn-instance-customerA] vpn-target 222:1 export-extcommunity
[PE1-vpn-instance-customerA] quit
```

On PE 1, create VPN instance **customerB** for Customer B.

```
[PE1] ip vpn-instance customerB
```

On PE 1, configure the RD as 200:1 for the VPN instance.

```
[PE1-vpn-instance-customerB] route-distinguisher 200:1
```

On PE 1, specify the import target and export target for the VPN instance as 333:1 and 444:1.

```
[PE1-vpn-instance-customerB] vpn-target 333:1 import-extcommunity
[PE1-vpn-instance-customerB] vpn-target 444:1 export-extcommunity
[PE1-vpn-instance-customerB] quit
```

On PE 1, associate VLAN-interface 100 with VPN instance **customerA**.

```
[PE1] vlan 100
[PE1-vlan100] port gigabitethernet 1/0/1
[PE1-vlan100] quit
[PE1] interface vlan-interface 100
[PE1-Vlan-interface100] ip binding vpn-instance customerA
[PE1-Vlan-interface100] ip address 100.1.1.2 24
[PE1-Vlan-interface100] quit
```

On PE 1, associate VLAN-interface 200 with VPN instance **customerB**.

```
[PE1] vlan 200
[PE1-vlan200] port gigabitethernet 1/0/3
[PE1-vlan200] quit
[PE1] interface vlan-interface 200
[PE1-Vlan-interface200] ip binding vpn-instance customerB
[PE1-Vlan-interface200] ip address 200.1.1.2 24
[PE1-Vlan-interface200] quit
```

On PE 2, create VPN instance **customerA** for Customer A.

```
[PE2] ip vpn-instance customerA
```

On PE 2, configure an RD for the VPN instance. HP recommends configuring the same RD as the one configured for VPN instance **customerA** on PE 1.

```
[PE2-vpn-instance-customerA] route-distinguisher 100:1
```

On PE 2, specify the import target and export target the same as the export target and import target on PE 1.

```
[PE2-vpn-instance-customerA] vpn-target 222:1 import-extcommunity
[PE2-vpn-instance-customerA] vpn-target 111:1 export-extcommunity
[PE2-vpn-instance-customerA] quit
```

On PE 2, create VPN instance **customerB** for Customer B.

```
[PE2] ip vpn-instance customerB
```

On PE 2, configure the RD as 200:1 for the VPN instance.

```
[PE2-vpn-instance-customerB] route-distinguisher 200:1
```

On PE 2, specify the import target and export target the same as the export target and import target on PE 1.

```
[PE2-vpn-instance-customerB] vpn-target 444:1 import-extcommunity
[PE2-vpn-instance-customerB] vpn-target 333:1 export-extcommunity
[PE2-vpn-instance-customerB] quit
```

On PE 2, associate VLAN-interface 101 with VPN instance **customerA**.

```
[PE2] vlan 101
[PE2-vlan101] port gigabitethernet 1/0/2
[PE2-vlan101] quit
[PE2] interface vlan-interface 101
[PE2-Vlan-interface101] ip binding vpn-instance customerA
[PE2-Vlan-interface101] ip address 101.1.1.1 24
[PE2-Vlan-interface101] quit
```

On PE 2, associate VLAN-interface 202 with VPN instance **customerB**.

```
[PE2] vlan 202
[PE2-vlan202] port gigabitethernet 1/0/3
[PE2-vlan202] quit
[PE2] interface vlan-interface 202
[PE2-Vlan-interface202] ip binding vpn-instance customerB
[PE2-Vlan-interface202] ip address 202.1.1.2 24
[PE2-Vlan-interface202] quit
```

Configure IP addresses for interfaces on the CEs, as shown in Figure 1. (Details not shown.)

Execute the **`display ip vpn-instance`** command on the PEs to display VPN instance configurations.

```
[PE1] display ip vpn-instance
  Total VPN-Instances configured : 2
  VPN-Instance Name               RD                     Create time
  customerA                       100:1                  2014/03/22 13:20:08
  customerB                       200:1                  2014/03/22 13:20:20
```

Use the **`ping`** command on the PEs to verify that the PEs can ping their attached CEs.

```
[PE1] ping -vpn-instance customerA 100.1.1.1
Ping 100.1.1.1 (100.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 100.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 100.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 100.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 100.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 100.1.1.1 in VPN instance customerA ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms
```

4. Establish EBGP peer relationships between PEs and CEs, and redistribute VPN routes into BGP:

On PE 1, create BGP process 100.

```
[PE1] bgp 100
```

On PE 1, specify CE 1 as a peer and redistribute direct routes of CE 1 into the BGP routing table of VPN instance **customerA**.

```
[PE1-bgp-default] ip vpn-instance customerA
[PE1-bgp-default-customerA] peer 100.1.1.1 as-number 65410
[PE1-bgp-default-customerA] address-family ipv4 unicast
[PE1-bgp-default-ipv4-customerA] peer 100.1.1.1 enable
[PE1-bgp-default-ipv4-customerA] import-route direct
[PE1-bgp-default-ipv4-customerA] quit
[PE1-bgp-default-customerA] quit
```

On PE 1, specify CE 2 as a peer and redistribute direct routes of CE 2 into the BGP routing table of VPN instance **customerB**.

```
[PE1-bgp-default] ip vpn-instance customerB
[PE1-bgp-default-customerB] peer 200.1.1.1 as-number 65410
[PE1-bgp-default-customerB] address-family ipv4 unicast
[PE1-bgp-default-ipv4-customerB] peer 200.1.1.1 enable
[PE1-bgp-default-ipv4-customerB] import-route direct
[PE1-bgp-default-ipv4-customerB] quit
[PE1-bgp-default-customerB] quit
[PE1-bgp-default] quit
```

On PE 2, create BGP process 100.

```
[PE2] bgp 100
```

On PE 2, specify CE 3 as a peer and redistribute direct routes of CE 3 into the BGP routing table of VPN instance **customerA**.

```
[PE2-bgp-default] ip vpn-instance customerA
[PE2-bgp-default-customerA] peer 101.1.1.2 as-number 65430
[PE2-bgp-default-customerA] address-family ipv4 unicast
[PE2-bgp-default-ipv4-customerA] peer 101.1.1.2 enable
[PE2-bgp-default-ipv4-customerA] import-route direct
[PE2-bgp-default-ipv4-customerA] quit
[PE2-bgp-default-customerA] quit
```

On PE 2, specify CE 4 as a peer and redistribute direct routes of CE 4 into the BGP routing table of VPN instance **customerB**.

```
[PE2-bgp-default] ip vpn-instance customerB
[PE2-bgp-default-customerB] peer 202.1.1.1 as-number 65430
[PE2-bgp-default-customerB] address-family ipv4 unicast
[PE2-bgp-default-ipv4-customerB] peer 202.1.1.1 enable
[PE2-bgp-default-ipv4-customerB] import-route direct
[PE2-bgp-default-ipv4-customerB] quit
[PE2-bgp-default-customerB] quit
[PE2-bgp-default] quit
```

On CE 1, create BGP process 65410, specify 100.1.1.2 as the peer, and specify the peer's AS number as 100.

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp-default] peer 100.1.1.2 as-number 100
```

On CE 1, enable BGP to exchange IPv4 unicast routing information with peer 100.1.1.2.

```
[CE1-bgp-default] address-family ipv4 unicast
[CE1-bgp-default-ipv4] peer 100.1.1.2 enable
```

On CE 1, redistribute the direct route for the site into EBGP.

```
[CE1-bgp-default-ipv4] import-route direct
[CE1-bgp-default-ipv4] quit
[CE1-bgp-default] quit
```

On CE 2, create BGP process 65410, specify 200.1.1.2 as the peer, and specify the peer's AS number as 100.

```
<CE2> system-view
[CE2] bgp 65410
[CE2-bgp-default] peer 200.1.1.2 as-number 100
```

On CE 2, enable BGP to exchange IPv4 unicast routing information with peer 200.1.1.2.

```
[CE2-bgp-default] address-family ipv4 unicast
[CE2-bgp-default-ipv4] peer 200.1.1.2 enable
```

On CE 2, redistribute the direct route for the site into EBGP.

```
[CE2-bgp-default-ipv4] import-route direct
[CE2-bgp-default-ipv4] quit
[CE2-bgp-default] quit
```

On CE 3, create BGP process 65430, specify 101.1.1.1 as the peer, and specify the peer's AS number as 100.

```
<CE3> system-view
[CE3] bgp 65430
[CE3-bgp-default] peer 101.1.1.1 as-number 100
```

On CE 3, enable BGP to exchange IPv4 unicast routing information with peer 101.1.1.1.

```
[CE3-bgp-default] address-family ipv4 unicast
[CE3-bgp-default-ipv4] peer 101.1.1.1 enable
```

On CE 3, redistribute the direct route for the site into EBGP.

```
[CE3-bgp-default-ipv4] import-route direct
[CE3-bgp-default-ipv4] quit
[CE3-bgp-default] quit
```

On CE 4, create BGP process 65430, specify 202.1.1.2 as the peer, and specify the peer's AS number as 100.

```
<CE4> system-view
[CE4] bgp 65430
[CE4-bgp-default] peer 202.1.1.2 as-number 100
```

On CE 4, enable BGP to exchange IPv4 unicast routing information with peer 202.1.1.2.

```
[CE4-bgp-default] address-family ipv4 unicast
[CE4-bgp-default-ipv4] peer 202.1.1.2 enable
```

On CE 4, redistribute the direct route for the site into EBGP.

```
[CE4-bgp-default-ipv4] import-route direct
[CE4-bgp-default-ipv4] quit
[CE4-bgp-default] quit
```

Verify that a BGP peer relationship in Established state has been established between a PE and a CE.

```
[PE1] display bgp peer ipv4 vpn-instance customerA

 BGP local router ID: 1.1.1.9
```

```
Local AS number: 100
Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

 100.1.1.1            65410        4        4    0       2 13:35:25 Established
```

5. Create an MP-IBGP peer relationship between PEs:

On PE 1, configure 3.3.3.9 as the BGP peer and specify Loopback 0 as the source interface for sending routing updates to the peer.

```
[PE1] bgp 100
[PE1-bgp-default] peer 3.3.3.9 as-number 100
[PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
```

On PE 1, enable the peer 3.3.3.9 for the BGP-VPNv4 address family.

```
[PE1-bgp-default] address-family vpnv4
[PE1-bgp-default-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-default-vpnv4] quit
[PE1-bgp-default] quit
```

On PE 2, configure 1.1.1.9 as the BGP peer and specify Loopback 0 as the source interface for sending routing updates to the peer.

```
[PE2] bgp 100
[PE2-bgp-default] peer 1.1.1.9 as-number 100
[PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
```

On PE 2, enable the peer 1.1.1.9 for the BGP-VPNv4 address family.

```
[PE2-bgp-default] address-family vpnv4
[PE2-bgp-default-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-default-vpnv4] quit
[PE2-bgp-default] quit
```

Verify that a BGP peer relationship in Established state has been established between the PEs.

```
[PE1] display bgp peer vpnv4

 BGP local router ID: 1.1.1.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

 * - Dynamically created peer
 Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

 3.3.3.9                100        8        8    0       0 00:00:08 Established
```

Verifying the configuration

Execute the **`display ip routing-table vpn-instance`** command on the PEs.

```
[PE1] display ip routing-table vpn-instance customerA

Destinations : 13        Routes : 13
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
100.1.1.0/24        Direct 0    0            100.1.1.2       Vlan100
100.1.1.0/32        Direct 0    0            100.1.1.2       Vlan100
100.1.1.2/32        Direct 0    0            127.0.0.1       InLoop0
100.1.1.255/32      Direct 0    0            100.1.1.2       Vlan100
101.1.1.0/24        BGP    255  0            3.3.3.9         Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0            0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0            0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0            127.0.0.1       InLoop0
```

The output shows that PE 1 has a route to the remote CE of Customer A. Output on PE 2 is similar.

Verify that CEs of the same VPN can ping each other, whereas those of different VPNs cannot. For example, CE 1 can ping CE 3 (101.1.1.2), but it cannot ping CE 4 (202.1.1.1). (Details not shown.)

Configuration files

- PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 import-extcommunity
 vpn-target 222:1 export-extcommunity
#
ip vpn-instance customerB
 route-distinguisher 200:1
 vpn-target 333:1 import-extcommunity
 vpn-target 444:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 100
#
vlan 200
#
mpls ldp
#
interface LoopBack0
```

```
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface100
 ip binding vpn-instance customerA
 ip address 100.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip binding vpn-instance customerB
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 200
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 3.3.3.9 enable
 #
 ip vpn-instance customerA
  peer 100.1.1.1 as-number 65410
  #
  address-family ipv4 unicast
   import-route direct
   peer 100.1.1.1 enable
 #
 ip vpn-instance customerB
  peer 200.1.1.1 as-number 65410
  #
  address-family ipv4 unicast
   import-route direct
   peer 200.1.1.1 enable
#
```

- P:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 5
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface5
 ip address 10.1.4.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 5
#
```

- PE 2:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 222:1 import-extcommunity
#
ip vpn-instance customerB
 route-distinguisher 200:1
 vpn-target 333:1 export-extcommunity
 vpn-target 444:1 import-extcommunity
```

```
#
ospf 1
 area 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 5
#
vlan 101
#
vlan 202
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface5
 ip address 10.1.4.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface101
 ip binding vpn-instance customerA
 ip address 101.1.1.1 255.255.255.0
#
interface Vlan-interface202
 ip binding vpn-instance customerB
 ip address 202.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 202
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 #
```

```
 address-family vpnv4
  peer 1.1.1.9 enable
 #
 ip vpn-instance customerA
  peer 101.1.1.2 as-number 65430
  #
  address-family ipv4 unicast
   import-route direct
   peer 101.1.1.2 enable
 #
 ip vpn-instance customerB
  peer 202.1.1.1 as-number 65430
  #
  address-family ipv4 unicast
   import-route direct
   peer 202.1.1.1 enable
#
```

- CE 1:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
bgp 65410
 peer 100.1.1.2 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
  peer 100.1.1.2 enable
#
```

- CE 2:

```
#
vlan 200
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
bgp 65410
 peer 200.1.1.2 as-number 100
```

```
 #
 address-family ipv4 unicast
  import-route direct
  peer 200.1.1.2 enable
#
```

- CE 3:

```
#
vlan 101
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
bgp 65430
 peer 101.1.1.1 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
  peer 101.1.1.1 enable
#
```

- CE 4:

```
#
vlan 202
#
interface Vlan-interface202
 ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 202
#
bgp 65430
 peer 202.1.1.2 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
  peer 202.1.1.2 enable
#
```

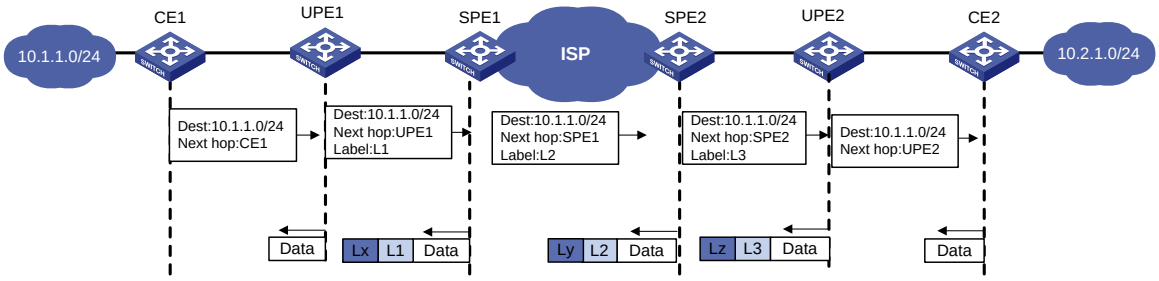
Example: Configuring HoVPN

Hierarchy of VPN (HoVPN) divides PEs into underlayer PEs (UPEs) or user-end PEs, and superstratum PEs (SPEs) or service provider-end PEs. UPEs and SPEs form a hierarchical PE structure.

UPEs and SPEs together provide the functions of a conventional PE.

- **UPE**—Provides user access. It maintains the routes of directly connected VPN sites. It does not maintain the routes of the remote sites in the VPN, or it only maintains their summary routes. A UPE assigns inner labels to the routes of its directly connected sites, and advertises the labels along with VPN routes to the SPE through MP-BGP.
- **SPE**—Manages and advertises VPN routes. It maintains all the routes of the VPNs connected through UPEs, including the routes of both the local and remote sites. An SPE advertises routes along with labels to UPEs, including the default routes of VPN instances or summary routes and the routes permitted by the routing policy. By using routing policies, you can control which sites in a VPN can communicate with each other.

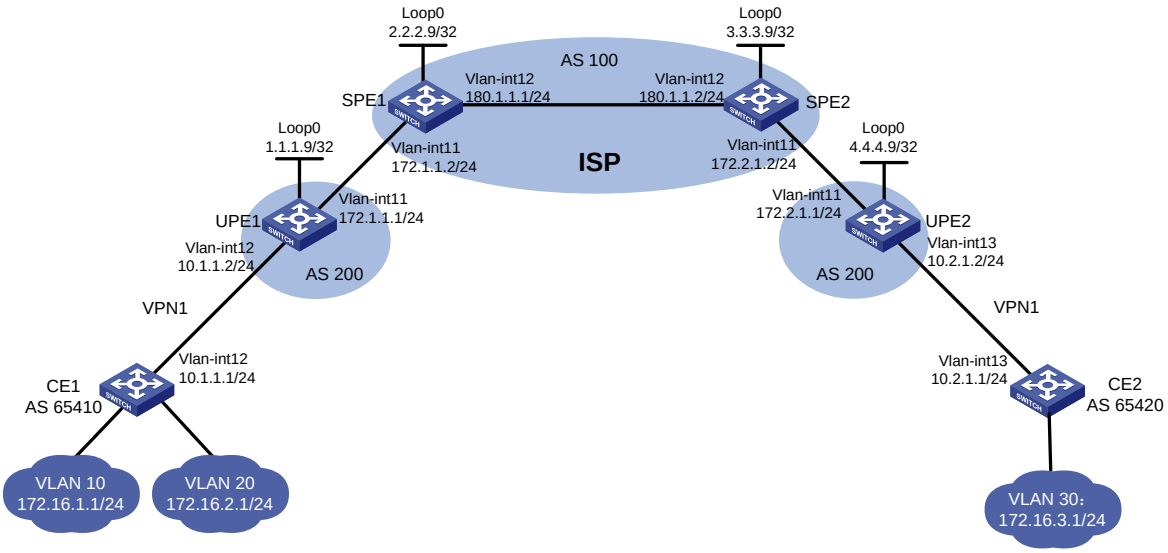
Figure 2 Routing process and label exchange for HoVPN



Network configuration

As shown in Figure 3, configure HoVPN and routing policies to allow communication between VLAN 10 and VLAN 30 and to disallow communication between VLAN 20 and VLAN 30.

Figure 3 Network diagram



Analysis

To ensure that VLAN 10 can communicate with VLAN 30 but VLAN 20 cannot, configure a routing policy on SPE 2 to advertise only the route of subnet 172.16.1.0/24 to UPE 2.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure HoVPN, follow these restrictions and guidelines:

- For an SPE to advertise routes to its connected UPE, perform the following configurations on the SPE:
  - Configure a routing policy to specify the routes that can be advertised.
  - Configure the BGP to advertise the routes permitted by the routing policy to the UPE.
- For an SPE and a UPE (EBGP peers) to advertise labels to each other, perform the following configurations:
  - Enable BGP to exchange labeled routes with the peer.
  - Configure a routing policy to specify the routes that can be advertised, and assign MPLS labels to the matching routes.
  - Apply the routing policy to routes outgoing to the peer.
- Associating an interface with a VPN instance deletes the IP address of the interface. You must reconfigure the IP address of the interface after the association. To avoid configuring the interface's IP address twice, configure the association first.

Procedures

1. Enable MPLS and MPLS LDP on SPEs, and configure the IGP protocol (OSPF, in this example):

On SPE 1, configure basic MPLS and MPLS LDP to establish LDP LSPs.

```
<SPE1> system-view
[SPE1] interface loopback 0
[SPE1-LoopBack0] ip address 2.2.2.9 32
[SPE1-LoopBack0] quit
[SPE1] mpls lsr-id 2.2.2.9
[SPE1] mpls ldp
[SPE1-ldp] quit
[SPE1] interface vlan-interface 11
[SPE1-Vlan-interface11] ip address 172.1.1.2 24
[SPE1-Vlan-interface11] mpls enable
[SPE1-Vlan-interface11] quit
[SPE1] interface vlan-interface 12
[SPE1-Vlan-interface12] ip address 180.1.1.1 24
[SPE1-Vlan-interface12] mpls enable
[SPE1-Vlan-interface12] mpls ldp enable
[SPE1-Vlan-interface12] quit
```

On SPE 1, configure OSPF.

```
[SPE1] ospf
[SPE1-ospf-1] area 0
[SPE1-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SPE1-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE1-ospf-1-area-0.0.0.0] quit
[SPE1-ospf-1] quit
```

On SPE 2, configure basic MPLS and MPLS LDP to establish LDP LSPs.

```
<SPE2> system-view
[SPE2] interface loopback 0
[SPE2-LoopBack0] ip address 3.3.3.9 32
[SPE2-LoopBack0] quit
[SPE2] mpls lsr-id 3.3.3.9
```

```
[SPE2] mpls ldp
[SPE2-ldp] quit
[SPE2] interface vlan-interface 12
[SPE2-Vlan-interface12] ip address 180.1.1.2 24
[SPE2-Vlan-interface12] mpls enable
[SPE2-Vlan-interface12] mpls ldp enable
[SPE2-Vlan-interface12] quit
[SPE2] interface vlan-interface 11
[SPE2-Vlan-interface11] ip address 172.2.1.2 24
[SPE2-Vlan-interface11] mpls enable
[SPE2-Vlan-interface11] quit
```

On SPE 2, configure OSPF.

```
[SPE2] ospf
[SPE2-ospf-1] area 0
[SPE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SPE2-ospf-1-area-0.0.0.0] network 180.1.1.0 0.0.0.255
[SPE2-ospf-1-area-0.0.0.0] quit
[SPE2-ospf-1] quit
```

Execute the **display mpls ldp peer** command to verify that an LDP session in Operational state has been established between the SPEs. (Details not shown.)

Execute the **display ospf peer** command to verify that an OSPF neighbor relationship in FULL state has been established between the SPEs. (Details not shown.)

2. Establish an MP-IBGP peer relationship between SPE 1 and SPE 2 to exchange VPNv4 routes:

On SPE 1, establish an MP-IBGP peer relationship with SPE 2.

```
[SPE1] bgp 100
[SPE1-bgp-default] peer 3.3.3.9 as-number 100
[SPE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[SPE1-bgp-default] address-family vpnv4
[SPE1-bgp-default-vpnv4] peer 3.3.3.9 enable
[SPE1-bgp-default-vpnv4] quit
[SPE1-bgp-default] quit
```

On SPE 2, establish an MP-IBGP peer relationship with SPE 1.

```
[SPE2] bgp 100
[SPE2-bgp-default] peer 2.2.2.9 as-number 100
[SPE2-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[SPE2-bgp-default] address-family vpnv4
[SPE2-bgp-default-vpnv4] peer 2.2.2.9 enable
[SPE2-bgp-default-vpnv4] quit
[SPE2-bgp-default] quit
```

Execute the **display bgp peer vpnv4** command on the SPEs to verify that a BGP peer relationship in Established state has been established. (Details not shown.)

3. Configure basic MPLS on UPEs:

Configure UPE 1.

```
<UPE1> system-view
[UPE1] interface loopback 0
[UPE1-LoopBack0] ip address 1.1.1.9 32
[UPE1-LoopBack0] quit
[UPE1] mpls lsr-id 1.1.1.9
```

```
[UPE1] interface vlan-interface 11
[UPE1-Vlan-interface11] ip address 172.1.1.1 24
[UPE1-Vlan-interface11] mpls enable
[UPE1-Vlan-interface11] quit
```

Configure UPE 2.

```
<UPE2> system-view
[UPE2] interface loopback 0
[UPE2-Loopback0] ip address 4.4.4.9 32
[UPE2-Loopback0] quit
[UPE2] mpls lsr-id 4.4.4.9
[UPE2] interface vlan-interface 11
[UPE2-Vlan-interface11] ip address 172.2.1.1 24
[UPE2-Vlan-interface11] mpls enable
[UPE2-Vlan-interface11] quit
```

4. Establish EBGP peer relationships between SPEs and UPEs, and enable them to exchange labeled routes to establish BGP LSPs:

Configure SPE 1.

```
[SPE1] bgp 100
[SPE1-bgp-default] peer 172.1.1.1 as-number 200
[SPE1-bgp-default] address-family ipv4
[SPE1-bgp-default-ipv4] peer 172.1.1.1 enable
[SPE1-bgp-default-ipv4] peer 172.1.1.1 label-route-capability
[SPE1-bgp-default-ipv4] peer 172.1.1.1 route-policy policy1 export
[SPE1-bgp-default-ipv4] network 2.2.2.9 255.255.255.255
[SPE1-bgp-default-ipv4] quit
[SPE1-bgp-default] quit
```

On SPE 1, configure routing policy **policy1** and set MPLS labels for routes.

```
[SPE1] route-policy policy1 permit node 0
[SPE1-route-policy-policy1-0] apply mpls-label
[SPE1-route-policy-policy1-0] quit
```

Configure UPE 1.

```
[UPE1] bgp 200
[UPE1-bgp-default] peer 172.1.1.2 as-number 100
[UPE1-bgp-default] address-family ipv4
[UPE1-bgp-default-ipv4] peer 172.1.1.2 enable
[UPE1-bgp-default-ipv4] peer 172.1.1.2 label-route-capability
[UPE1-bgp-default-ipv4] peer 172.1.1.2 route-policy policy1 export
[UPE1-bgp-default-ipv4] network 1.1.1.9 255.255.255.255
[UPE1-bgp-default-ipv4] quit
[UPE1-bgp-default] quit
```

On UPE 1, configure routing policy **policy1** and set MPLS labels for routes.

```
[UPE1] route-policy policy1 permit node 0
[UPE1-route-policy-policy1-0] apply mpls-label
[UPE1-route-policy-policy1-0] quit
```

Configure SPE 2.

```
[SPE2] bgp 100
[SPE2-bgp-default] peer 172.2.1.1 as-number 200
[SPE2-bgp-default] address-family ipv4
```

```
[SPE2-bgp-default-ipv4] peer 172.2.1.1 enable
[SPE2-bgp-default-ipv4] peer 172.2.1.1 label-route-capability
[SPE2-bgp-default-ipv4] peer 172.2.1.1 route-policy policy1 export
[SPE2-bgp-default-ipv4] network 3.3.3.9 255.255.255.255
[SPE2-bgp-default-ipv4] quit
[SPE2-bgp-default] quit
```

On SPE 2, configure routing policy **policy1** and set MPLS labels for routes.

```
[SPE2] route-policy policy1 permit node 0
[SPE2-route-policy-policy1-0] apply mpls-label
[SPE2-route-policy-policy1-0] quit
```

Configure UPE 2.

```
[UPE2] bgp 200
[UPE2-bgp-default] peer 172.2.1.2 as-number 100
[UPE2-bgp-default] address-family ipv4
[UPE2-bgp-default-ipv4] peer 172.2.1.2 enable
[UPE2-bgp-default-ipv4] peer 172.2.1.2 label-route-capability
[UPE2-bgp-default-ipv4] peer 172.2.1.2 route-policy policy1 export
[UPE2-bgp-default-ipv4] network 4.4.4.9 255.255.255.255
[UPE2-bgp-default-ipv4] quit
[UPE2-bgp-default] quit
```

On UPE 2, configure routing policy **policy1** and set MPLS labels for routes.

```
[UPE2] route-policy policy1 permit node 0
[UPE2-route-policy-policy1-0] apply mpls-label
[UPE2-route-policy-policy1-0] quit
```

Execute the **display mpls lsp** command on the SPEs and UPEs to verify that BGP LSPs have been established between each SPE and its connected UPE. (Details not shown.)

5. Establish MP-EBGP peer relationships between SPEs and UPEs, and configure HoVPN:

On UPE 1, establish an MP-EBGP peer relationship with SPE 1.

```
[UPE1] bgp 200
[UPE1-bgp-default] peer 2.2.2.9 as-number 100
[UPE1-bgp-default] peer 2.2.2.9 connect-interface loopback 0
[UPE1-bgp-default] address-family vpnv4
[UPE1-bgp-default-vpnv4] peer 2.2.2.9 enable
```

On UPE 1, allow the local AS number to appear in the AS_PATH attribute of the routes received.

```
[UPE1-bgp-default-vpnv4] peer 2.2.2.9 allow-as-loop
[UPE1-bgp-default-vpnv4] quit
```

On SPE 1, configure VPN instance **vpn1**.

```
[SPE1] ip vpn-instance vpn1
[SPE1-vpn-instance-vpn1] route-distinguisher 100:1
[SPE1-vpn-instance-vpn1] vpn-target 100:1 both
[SPE1-vpn-instance-vpn1] quit
```

On SPE 1, establish an MP-EBGP peer relationship with UPE 1, and specify UPE 1 as a UPE.

```
[SPE1] bgp 100
[SPE1-bgp-default] peer 1.1.1.9 as-number 200
[SPE1-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[SPE1-bgp-default] address-family vpnv4
[SPE1-bgp-default-vpnv4] peer 1.1.1.9 enable
```

```
[SPE1-bgp-default-vpnv4] peer 1.1.1.9 upe
[SPE1-bgp-default-vpnv4] quit
```

On SPE 1, create a BGP-VPN instance so the learned VPNv4 routes can be added into the BGP routing table of the VPN instance.

```
[SPE1-bgp-default] ip vpn-instance vpn1
[SPE1-bgp-default-vpn1] quit
[SPE1-bgp-default] quit
```

On UPE 2, establish an MP-EBGP peer relationship with SPE 2.

```
[UPE2] bgp 200
[UPE2-bgp-default] peer 3.3.3.9 as-number 100
[UPE2-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[UPE2-bgp-default] address-family vpnv4
[UPE2-bgp-default-vpnv4] peer 3.3.3.9 enable
```

On UPE 2, allow the local AS number to appear in the AS_PATH attribute of the routes received.

```
[UPE2-bgp-default-vpnv4] peer 3.3.3.9 allow-as-loop
[UPE2-bgp-default-vpnv4] quit
```

On SPE 2, configure VPN instance **vpn1**.

```
[SPE2] ip vpn-instance vpn1
[SPE2-vpn-instance-vpn1] route-distinguisher 100:1
[SPE2-vpn-instance-vpn1] vpn-target 100:1 both
[SPE2-vpn-instance-vpn1] quit
```

On SPE 2, establish an MP-EBGP peer relationship with UPE 2, and specify UPE 2 as a UPE.

```
[SPE2] bgp 100
[SPE2-bgp-default] peer 4.4.4.9 as-number 200
[SPE2-bgp-default] peer 4.4.4.9 connect-interface loopback 0
[SPE2-bgp-default] address-family vpnv4
[SPE2-bgp-default-vpnv4] peer 4.4.4.9 enable
[SPE2-bgp-default-vpnv4] peer 4.4.4.9 upe
[SPE2-bgp-default-vpnv4] quit
```

On SPE 2, create a BGP-VPN instance so the learned VPNv4 routes can be added into the BGP routing table of the VPN instance.

```
[SPE2-bgp-default] ip vpn-instance vpn1
[SPE2-bgp-default-vpn1] quit
[SPE2-bgp-default] quit
```

Execute the **`display bgp peer vpnv4`** command on the SPEs and UPEs to verify that a BGP peer relationship in Established state has been established between each SPE and its connected UPE. (Details not shown.)

6. Allow CE access to UPEs:

On UPE 1, configure VPN instance **vpn1** to allow CE 1 to access UPE 1.

```
[UPE1] ip vpn-instance vpn1
[UPE1-vpn-instance-vpn1] route-distinguisher 100:1
[UPE1-vpn-instance-vpn1] vpn-target 100:1 both
[UPE1-vpn-instance-vpn1] quit
[UPE1] interface vlan-interface 12
[UPE1-Vlan-interface12] ip binding vpn-instance vpn1
[UPE1-Vlan-interface12] ip address 10.1.1.2 24
[UPE1-Vlan-interface12] quit
```

On UPE 1, establish an EBGP peer relationship with CE 1, and redistribute VPN routes into BGP.

```
[UPE1] bgp 200
[UPE1-bgp-default] ip vpn-instance vpn1
[UPE1-bgp-default-vpn1] peer 10.1.1.1 as-number 65410
[UPE1-bgp-default-vpn1] address-family ipv4 unicast
[UPE1-bgp-default-ipv4-vpn1] peer 10.1.1.1 enable
[UPE1-bgp-default-ipv4-vpn1] import-route direct
[UPE1-bgp-default-ipv4-vpn1] quit
[UPE1-bgp-default-vpn1] quit
```

On CE 1, establish an EBGP peer relationship with UPE 1, and redistribute direct routes into BGP.

```
<CE1> system-view
[CE1] interface vlan-interface 12
[CE1-Vlan-interface12] ip address 10.1.1.1 255.255.255.0
[CE1-Vlan-interface12] quit
[CE1] bgp 65410
[CE1-bgp-default] peer 10.1.1.2 as-number 200
[CE1-bgp-default] address-family ipv4 unicast
[CE1-bgp-default-ipv4] peer 10.1.1.2 enable
[CE1-bgp-default-ipv4] import-route direct
[CE1-bgp-default-ipv4] quit
[CE1-bgp-default] quit
```

On UPE 2, configure VPN instance **vpn1** to allow CE 2 to access UPE 2.

```
[UPE2] ip vpn-instance vpn1
[UPE2-vpn-instance-vpn1] route-distinguisher 100:1
[UPE2-vpn-instance-vpn1] vpn-target 100:1 both
[UPE2-vpn-instance-vpn1] quit
[UPE2] interface vlan-interface 12
[UPE2-Vlan-interface12] ip binding vpn-instance vpn1
[UPE2-Vlan-interface12] ip address 10.2.1.2 24
[UPE2-Vlan-interface12] quit
```

On UPE 2, establish an EBGP peer relationship with CE 2, and redistribute VPN routes into BGP.

```
[UPE2] bgp 200
[UPE2-bgp-default] ip vpn-instance vpn1
[UPE2-bgp-default-vpn1] peer 10.2.1.1 as-number 65420
[UPE2-bgp-default-vpn1] address-family ipv4 unicast
[UPE2-bgp-default-ipv4-vpn1] peer 10.2.1.1 enable
[UPE2-bgp-default-ipv4-vpn1] import-route direct
[UPE2-bgp-default-ipv4-vpn1] quit
[UPE2-bgp-default-vpn1] quit
```

On CE 2, establish an EBGP peer relationship with UPE 2, and redistribute direct routes into BGP.

```
<CE2> system-view
[CE2] interface vlan-interface 12
[CE2-Vlan-interface12] ip address 10.2.1.1 255.255.255.0
[CE2-Vlan-interface12] quit
[CE2] bgp 65420
```

```
[CE2-bgp-default] peer 10.2.1.2 as-number 200
[CE2-bgp-default] address-family ipv4 unicast
[CE2-bgp-default-ipv4] peer 10.2.1.2 enable
[CE2-bgp-default-ipv4] import-route direct
[CE2-bgp-default-ipv4] quit
[CE2-bgp-default] quit
```

Execute the **display bgp peer ipv4** command on the UPEs and CEs to verify that a BGP peer relationship in Established state has been established between each UPE and its connected CE. (Details not shown.)

7. Configure routing policies on SPEs to filter VPN routes to be advertised:

On SPE 1, advertise the routes permitted by routing policy policy2 (the routes of CE 2) to UPE 1.

```
[SPE1] ip prefix-list list1 index 10 permit 172.16.3.0 24
[SPE1] route-policy policy2 permit node 0
[SPE1-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE1-route-policy-policy2-0] quit
[SPE1] bgp 100
[SPE1-bgp-default] address-family vpnv4
[SPE1-bgp-default-vpnv4] peer 1.1.1.9 upe route-policy policy2 export
```

On SPE 2, advertise the routes permitted by routing policy policy2 (the routes of subnet 172.16.1.0 connected to CE 1) to UPE 2.

```
[SPE2] ip prefix-list list1 index 10 permit 172.16.1.0 24
[SPE2] route-policy policy2 permit node 0
[SPE2-route-policy-policy2-0] if-match ip address prefix-list list1
[SPE2-route-policy-policy2-0] quit
[SPE2] bgp 100
[SPE2-bgp-default] address-family vpnv4
[SPE2-bgp-default-vpnv4] peer 4.4.4.9 upe route-policy policy2 export
```

Verifying the configuration

Verify that CE 1 has learned the route to subnet 172.16.3.0/24 of CE 2.

```
[CE1]display ip routing-table

Destinations : 25        Routes : 25

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
172.16.1.0/24       Direct 0    0            172.16.1.1      VLAN10
172.16.1.0/32       Direct 0    0            172.16.1.1      VLAN10
172.16.1.1/32       Direct 0    0            127.0.0.1       InLoop0
172.16.1.255/32     Direct 0    0            172.16.1.1      VLAN10
172.16.2.0/24       Direct 0    0            172.16.2.1      VLAN20
172.16.2.0/32       Direct 0    0            172.16.2.1      VLAN20
172.16.2.1/32       Direct 0    0            127.0.0.1       InLoop0
172.16.2.255/32     Direct 0    0            172.16.2.1      VLAN20
172.16.3.0/24       BGP    255  0            10.1.1.2        VLAN12
```

Verify that CE 2 has learned the route to subnet 172.16.1.0/24 of CE 1, but it has not learned the route to 172.16.2.0/24 of CE 1.

```
[CE2] display ip routing-table

Destinations : 21        Routes : 21

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
172.16.1.0/24       BGP    255  0            10.2.1.2        VLAN13
172.16.3.0/24       Direct 0    0            172.16.3.1      VLAN30
172.16.3.0/32       Direct 0    0            172.16.3.1      VLAN30
172.16.3.1/32       Direct 0    0            127.0.0.1       InLoop0
172.16.3.255/32     Direct 0    0            172.16.3.1      VLAN30
```

Verify that VLAN 10 and VLAN 30 can ping each other, and VLAN 20 and VLAN 30 cannot ping each other. (Details not shown.)

Configuration files

- CE 1:

```
#
vlan 10
#
vlan 12
#
vlan 20
#
interface Vlan-interface10
 ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface12
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 172.16.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 12
#
bgp 65410
 peer 10.1.1.2 as-number 200
 #
 address-family ipv4 unicast
```

```
  import-route direct
  peer 10.1.1.2 enable
#
```

- CE 2:

```
#
vlan 13
#
vlan 30
#
interface Vlan-interface13
ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface30
ip address 172.16.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
bgp 65420
 peer 10.2.1.2 as-number 200
 #
 address-family ipv4 unicast
  import-route direct
  peer 10.2.1.2 enable
#
```

- UPE 1:

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 mpls lsr-id 1.1.1.9
#
vlan 11 to 12
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface11
ip address 172.1.1.1 255.255.255.0
 mpls enable
#
```

```
interface Vlan-interface12
ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
bgp 200
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
 peer 172.1.1.2 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
  network 1.1.1.9 255.255.255.255
  network 172.1.1.0 255.255.255.0
  peer 172.1.1.2 enable
  peer 172.1.1.2 route-policy hope export
  peer 172.1.1.2 label-route-capability
 #
 address-family vpnv4
  peer 2.2.2.9 enable
  peer 2.2.2.9 allow-as-loop 1
 #
 ip vpn-instance vpn1
  peer 10.1.1.1 as-number 65410
  #
  address-family ipv4 unicast
   import-route direct
   peer 10.1.1.1 enable
#
route-policy hope permit node 0
 apply mpls-label
#
```

- SPE 1:

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
```

```
  network 2.2.2.9 0.0.0.0
  network 180.1.1.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
vlan 11 to 12
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface11
 ip address 172.1.1.2 255.255.255.0
 mpls enable
#
interface Vlan-interface12
 ip address 180.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
bgp 100
 peer 1.1.1.9 as-number 200
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 172.1.1.1 as-number 200
 #
 address-family ipv4 unicast
  network 2.2.2.9 255.255.255.255
  peer 172.1.1.1 enable
  peer 172.1.1.1 route-policy policy1 export
  peer 172.1.1.1 label-route-capability
 #
 address-family vpnv4
  peer 1.1.1.9 enable
  peer 1.1.1.9 upe
  peer 1.1.1.9 upe route-policy policy2 export
  peer 3.3.3.9 enable
 #
```

```
 ip vpn-instance vpn1
#
route-policy policy1 permit node 0
 apply mpls-label
#
route-policy policy2 permit node 0
 if-match ip address prefix-list list1
#
 ip prefix-list list1 index 10 permit 172.16.3.0 24
#
```

- UPE 2:

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 mpls lsr-id 4.4.4.9
#
vlan 11
#
vlan 13
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface11
 ip address 172.2.1.1 255.255.255.0
 mpls enable
#
interface Vlan-interface13
 ip binding vpn-instance vpn1
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
bgp 200
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 172.2.1.2 as-number 100
 #
 address-family ipv4 unicast
```

```
  network 4.4.4.9 255.255.255.255
  peer 172.2.1.2 enable
  peer 172.2.1.2 route-policy hope export
  peer 172.2.1.2 label-route-capability
 #
 address-family vpnv4
  peer 3.3.3.9 enable
  peer 3.3.3.9 allow-as-loop 1
 #
 ip vpn-instance vpn1
  peer 10.2.1.1 as-number 65420
  #
  address-family ipv4 unicast
   import-route direct
   peer 10.2.1.1 enable
#
route-policy hope permit node 0
 apply mpls-label
#
```

- SPE 2:

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 180.1.1.0 0.0.0.255
#
 mpls lsr-id 3.3.3.9
#
vlan 11 to 12
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface11
 ip address 172.2.1.2 255.255.255.0
mpls enable
#
interface Vlan-interface12
 ip address 180.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
bgp 100
 router-id 3.3.3.9
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 200
 peer 4.4.4.9 connect-interface LoopBack0
 peer 172.2.1.1 as-number 200
 #
 address-family ipv4 unicast
  network 3.3.3.9 255.255.255.255
  peer 172.2.1.1 enable
  peer 172.2.1.1 route-policy policy1 export
  peer 172.2.1.1 label-route-capability
 #
 address-family vpnv4
  peer 2.2.2.9 enable
  peer 4.4.4.9 enable
  peer 4.4.4.9 upe
  peer 4.4.4.9 upe route-policy policy2 export
 #
 ip vpn-instance vpn1
#
route-policy policy1 permit node 0
 apply mpls-label
#
route-policy policy2 permit node 0
 if-match ip address prefix-list list1
#
 ip prefix-list list1 index 10 permit 172.16.1.0 24
#
```

Contents

Introduction

This document provides MPLS Operation, Administration, and Maintenance (OAM) configuration examples.

MPLS OAM provides the following fault management tools for LSPs:

- MPLS data plane connectivity verification.
- MPLS data plane and control plane consistency verification.
- Failure detection and locating.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MPLS OAM.

Example: Configuring BFD for an LSP

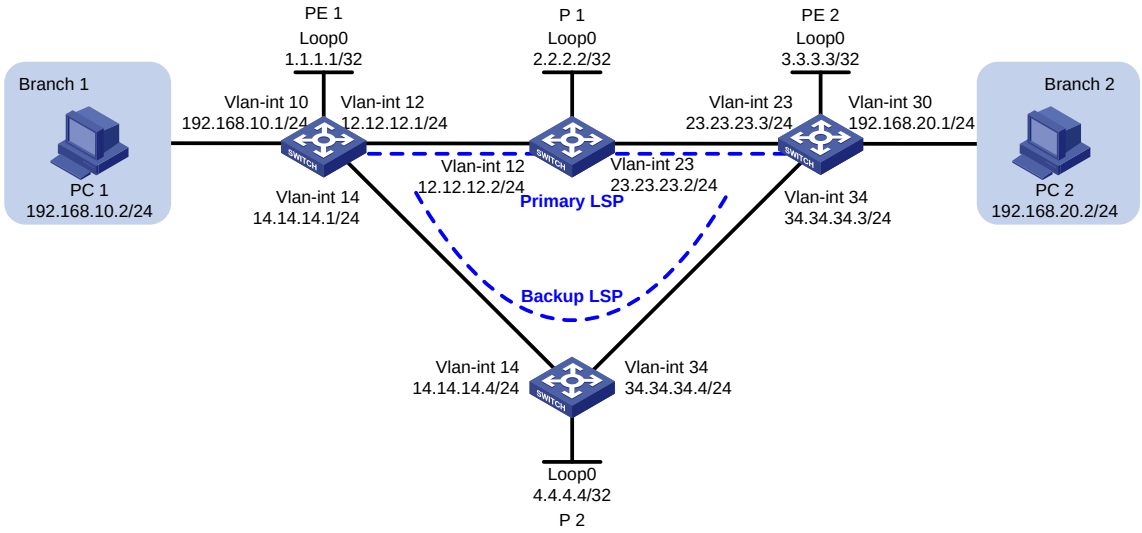
Network configuration

As shown in Figure 1, a company has two branches that are connected to the MPLS backbone. It requires the MPLS backbone to establish LSPs for communication between the branches, and to provide high availability services for uninterrupted business between the branches.

To meet the requirements:

- Establish LSPs by using LDP.
- Configure OSPF FRR on the MPLS backbone so LDP can establish a primary LSP and a backup LSP.
- Configure BFD for the primary LSP. When the primary LSP fails, BFD can quickly detect the failure and notify LDP of the failure, so LDP can immediately switch traffic to the backup LSP.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx switch series, Release 6628Pxx switch series
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628P
S5560X-HI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5500V2-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30F switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 65xx switch series, Release 6628Pxx switch series
S6520X-SI switch series S6520-SI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 65xx switch series, Release 6628Pxx switch series

Hardware	Software version
S5000-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4600 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
ES5500 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI.

Procedures

1. Configure IP addresses for interfaces:

   # On PE 1, configure IP addresses and masks for interfaces, including the loopback interface, as shown in Figure 1.

```
<PE1> system-view
[PE1] vlan 10
[PE1-vlan10] port gigabitethernet 1/0/3
[PE1-vlan10] quit
[PE1] interface vlan-interface 10
[PE1-Vlan-interface10] ip address 192.168.10.1 24
[PE1] vlan 12
[PE1-vlan12] port gigabitethernet 1/0/1
[PE1-vlan12] quit
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 12.12.12.1 24
[PE1-Vlan-interface12] quit
[PE1] vlan 14
[PE1-vlan14] port gigabitethernet 1/0/2
[PE1-vlan14] quit
[PE1] interface vlan-interface 14
[PE1-Vlan-interface14] ip address 14.14.14.1 24
[PE1-Vlan-interface14] quit
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 1.1.1.1 32
[PE1-LoopBack0] quit
```

Configure other devices in the same way that PE 1 is configured. (Details not shown.)

2. Configure OSPF to ensure IP connectivity within the MPLS backbone, and enable OSPF FRR:

Configure PE 1.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] fast-reroute lfa
[PE1-ospf-1] quit
```

Configure P 1.

```
[P1] ospf
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

Configure PE 2.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 34.34.34..0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] fast-reroute lfa
[PE2-ospf-1] quit
```

Configure P 2.

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

On P 2, set the OSPF cost to 10 for VLAN-interface 14 and VLAN-interface 34. This setting ensures that the backup LSP has a larger OSPF cost than the primary LSP.

```
[P2] interface vlan-interface 14
[P2-Vlan-interface14] ospf cost 10
[P2-Vlan-interface14] quit
[P2] interface vlan-interface 34
[P2-Vlan-interface34] ospf cost 10
[P2-Vlan-interface34] quit
```

3. Configure basic MPLS and MPLS LDP:

Configure PE 1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
[PE1] interface vlan-interface 14
[PE1-Vlan-interface14] mpls enable
[PE1-Vlan-interface14] mpls ldp enable
[PE1-Vlan-interface14] quit
```

Configure P 1.

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
[P1-ldp] quit
[P1] interface vlan-interface 12
[P1-Vlan-interface12] mpls enable
[P1-Vlan-interface12] mpls ldp enable
[P1-Vlan-interface12] quit
[P1] interface vlan-interface 23
[P1-Vlan-interface23] mpls enable
[P1-Vlan-interface23] mpls ldp enable
[P1-Vlan-interface23] quit
```

Configure PE 2.

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface vlan-interface 23
[PE2-Vlan-interface23] mpls enable
[PE2-Vlan-interface23] mpls ldp enable
[PE2-Vlan-interface23] quit
[PE2] interface vlan-interface 34
[PE2-Vlan-interface34] mpls enable
[PE2-Vlan-interface34] mpls ldp enable
[PE2-Vlan-interface34] quit
```

Configure P 2.

```
[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface vlan-interface 14
[P2-Vlan-interface14] mpls enable
[P2-Vlan-interface14] mpls ldp enable
[P2-Vlan-interface14] quit
[P2] interface vlan-interface 34
[P2-Vlan-interface34] mpls enable
[P2-Vlan-interface34] mpls ldp enable
```

```
[P2-Vlan-interface34] quit
```

Verify that LDP sessions in **Operational** state have been established on each device. The following shows the output on PE 1.

```
[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID            State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.2:0              Operational   Passive  Off  Off  55/55
4.4.4.4:0              Operational   Passive  Off  Off  6/6
```

4. Configure LSP generation policies to establish LSPs to destinations 192.168.10.0/24, 192.168.20.0/24, 1.1.1.1/32, and 3.3.3.3/32:

On PE 1, create IP prefix list **PE1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE1] ip prefix-list PE1 index 10 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 20 permit 192.168.20.0 24
[PE1] ip prefix-list PE1 index 30 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 40 permit 3.3.3.3 32
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

On P 1, create IP prefix list **P1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P1] ip prefix-list P1 index 10 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 20 permit 192.168.20.0 24
[P1] ip prefix-list P1 index 30 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 40 permit 3.3.3.3 32
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

On PE 2, create IP prefix list **PE2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE2] ip prefix-list PE2 index 10 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 20 permit 192.168.20.0 24
[PE2] ip prefix-list PE2 index 30 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 40 permit 3.3.3.3 32
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

On P 2, create IP prefix list **P2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P2] ip prefix-list P2 index 10 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 20 permit 192.168.20.0 24
[P2] ip prefix-list P2 index 30 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 40 permit 3.3.3.3 32
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

Verify that LSPs to destination 192.168.20.0/24 have been established on PE 1. The primary LSP uses VLAN-interface 12 as the outgoing interface and the backup LSP uses VLAN-interface 14 as the outgoing interface.

```
[PE1]display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
Statistics:
  FECs: 4      Ingress LSPs: 4     Transit LSPs: 4     Egress LSPs: 2

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1279(L)
3.3.3.3/32         -/1150              12.12.12.2      Vlan12
                   1150/1150           12.12.12.2      Vlan12
                   -/1150(B)           12.12.12.2      Vlan14
                   1150/1150(B)        12.12.12.2      Vlan14
192.168.10.0/24    1141/-
                   -/1141(L)
                   -/1141(L)
192.168.20.0/24    -/1133              12.12.12.2      Vlan12
                   1133/1133           12.12.12.2      Vlan12
                   -/1133(B)           14.14.14.4      Vlan14
                   1133/1133(B)        14.14.14.4      Vlan14
```

5. Enable BFD for MPLS and use BFD to verify LSP connectivity:

Configure PE 1.

```
[PE1] mpls bfd enable
[PE1] mpls bfd 3.3.3.3 32
```

Configure PE 2.

```
[PE2] mpls bfd enable
[PE2] mpls bfd 1.1.1.1 32
```

Verifying the configuration

1. Display BFD information for LSPs on PE 1 and PE 2. The following shows the output on PE 1.

```
[PE1] display mpls bfd
 Total number of sessions: 2, 2 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 1.1.1.1
   Mask Length: 32
 NHLFE ID: -
 Local Discr: 1026                  Remote Discr: 514
 Source IP: 1.1.1.1                 Destination IP: 3.3.3.3
 Session State: Up                  Session Role: Active
 Template Name: -

 FEC Type: LSP
 FEC Info:
   Destination: 3.3.3.3
   Mask Length: 32
```

```
NHLFE ID: 1028
Local Discr: 1025                    Remote Discr: -
Source IP: 1.1.1.1                   Destination IP: 127.0.0.1
Session State: Up                    Session Role: Passive
Template Name: -
```

2. Execute the **tracert mpls ipv4** command on PE 1. The output shows that the primary LSP is in use.

NOTE:

Before you use the tracert feature, enable sending ICMP time exceeded messages on intermediate devices, and enable sending ICMP destination unreachable messages on the destination device.

```
[PE1] tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   12.12.12.2/[1148]
  1     12.12.12.2         2 ms    Transit   23.23.23.3/[1148]
  2     23.23.23.3         2 ms    Egress
```

3. Verify that the ping operation from PE 1 to PE 2 will not fail after VLAN-interface 23 on P 1 is shut down during the ping operation:

   # Ping PE 2 from PE 1.

```
[PE1] ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
…
```

   # Shut down VLAN-interface 23 on P 1.

```
[P1] interface vlan-interface 23
[P1-Vlan-interface23] shutdown
```

   # View the **ping** command output. The output shows that the communication was interrupted, and then immediately resumed.

```
[PE1] ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
…
56 bytes from 192.168.20.1: icmp_seq=7 ttl=254 time=2.214 ms
Request time out
56 bytes from 192.168.20.1: icmp_seq=9 ttl=254 time=2.659 ms
56 bytes from 192.168.20.1: icmp_seq=10 ttl=254 time=5.049 ms
56 bytes from 192.168.20.1: icmp_seq=11 ttl=254 time=2.098 ms
56 bytes from 192.168.20.1: icmp_seq=12 ttl=254 time=2.225 ms
56 bytes from 192.168.20.1: icmp_seq=13 ttl=254 time=2.187 ms

--- Ping statistics for 192.168.20.1 ---
14 packet(s) transmitted, 13 packet(s) received, 7.1% packet loss
```

```
round-trip min/avg/max/std-dev = 1.990/2.455/5.049/0.772 ms
```

4. Execute the **`tracert mpls ipv4`** command on PE 1. The output shows that the backup LSP is in use.

```
[PE1] tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   14.14.14.4/[1276]
  1     14.14.14.4         2 ms    Transit   34.34.34.3/[1148]
  2     34.34.34.3         2 ms    Egress
```

Configuration files

- PE 1:

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
vlan 10
#
vlan 12
#
vlan 14
#
mpls ldp
 lsp-trigger prefix-list PE1
#
 mpls bfd enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface14
 ip address 14.14.14.1 255.255.255.0
```

```
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 14
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
 ip prefix-list PE1 index 10 permit 192.168.10.0 24
 ip prefix-list PE1 index 20 permit 192.168.20.0 24
 ip prefix-list PE1 index 30 permit 1.1.1.1 32
 ip prefix-list PE1 index 40 permit 3.3.3.3 32
#
 mpls bfd 3.3.3.3 32
#
```

- PE 2:

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
vlan 23
#
vlan 30
#
vlan 34
#
 mpls lsr-id 3.3.3.3
#
mpls ldp
 lsp-trigger prefix-list PE2
#
 mpls bfd enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
```

```
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface30
 ip address 192.168.20.1 255.255.255.0
#
interface Vlan-interface34
 ip address 34.34.34.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 34
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 23
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
 ip prefix-list PE2 index 10 permit 192.168.10.0 24
 ip prefix-list PE2 index 20 permit 192.168.20.0 24
 ip prefix-list PE2 index 30 permit 1.1.1.1 32
 ip prefix-list PE2 index 40 permit 3.3.3.3 32
#
 mpls bfd 1.1.1.1 32
#
```

- P 1:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
vlan 12
#
vlan 23
#
mpls ldp
 lsp-trigger prefix-list P1
```

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface23
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 23
#
 ip prefix-list P1 index 10 permit 192.168.10.0 24
 ip prefix-list P1 index 20 permit 192.168.20.0 24
 ip prefix-list P1 index 30 permit 1.1.1.1 32
 ip prefix-list P1 index 40 permit 3.3.3.3 32
#
```

- P 2:

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
vlan 14
#
vlan 34
#
mpls ldp
 lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface14
```

```
 ip address 14.14.14.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface Vlan-interface34
 ip address 34.34.34.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 34
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 14
#
 ip prefix-list P2 index 10 permit 192.168.10.0 24
 ip prefix-list P2 index 20 permit 192.168.20.0 24
 ip prefix-list P2 index 30 permit 1.1.1.1 32
 ip prefix-list P2 index 40 permit 3.3.3.3 32
#
```

Example: Configuring SBFD for an LSP

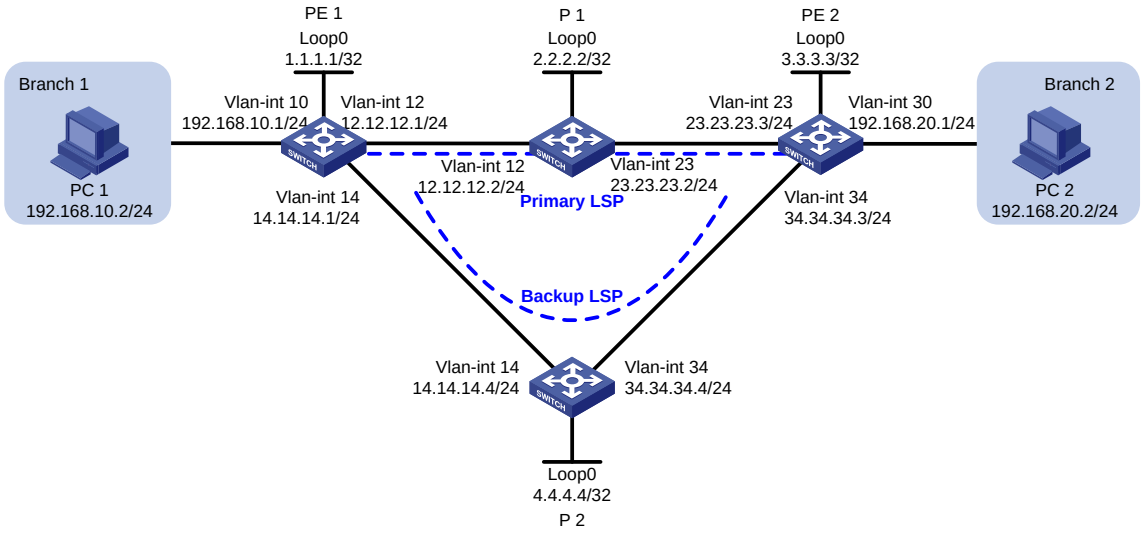
Network configuration

As shown in Figure 2, a company has two branches that are connected to the MPLS backbone. It requires the MPLS backbone to establish LSPs for communication between the branches, and to provide high availability services for uninterrupted business between the branches.

To meet the requirements:

- Establish LSPs by using LDP.
- Configure OSPF FRR on the MPLS backbone so LDP can establish a primary LSP and a backup LSP.
- Configure SBFD for the primary LSP. When the primary LSP fails, SBFD can quickly detect the failure and notify LDP of the failure, so LDP can immediately switch traffic to the backup LSP.

Figure 2 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx switch series, Release 6628Pxx switch series
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5560X-HI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
S5500V2-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx
MS4520V2-30F switch	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx switch series, Release 6628Pxx switch series
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S6520X-SI switch series S6520-SI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series

Hardware	Software version
ES5500 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
MS4600 switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5000-EI switch series	Release 65xx switch series, Release 6615Pxx switch series, Release 6628Pxx switch series
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported

Hardware	Software version
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switches IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI.

Procedures

1. Configure IP addresses for interfaces:

   # On PE 1, configure IP addresses and masks for interfaces, including the loopback interface, as shown in Figure 2.

```
<PE1> system-view
[PE1] vlan 10
[PE1-vlan10] port gigabitethernet 1/0/3
[PE1-vlan10] quit
[PE1] interface vlan-interface 10
[PE1-Vlan-interface10] ip address 192.168.10.1 24
[PE1] vlan 12
[PE1-vlan12] port gigabitethernet 1/0/1
[PE1-vlan12] quit
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 12.12.12.1 24
[PE1-Vlan-interface12] quit
[PE1] vlan 14
[PE1-vlan14] port gigabitethernet 1/0/2
[PE1-vlan14] quit
[PE1] interface vlan-interface 14
[PE1-Vlan-interface14] ip address 14.14.14.1 24
[PE1-Vlan-interface14] quit
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 1.1.1.1 32
[PE1-LoopBack0] quit
```

2. Configure OSPF to ensure IP connectivity within the MPLS backbone, and enable OSPF FRR:

Configure PE 1.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] fast-reroute lfa
[PE1-ospf-1] quit
```

Configure P 1.

```
[P1] ospf
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

Configure PE 2.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 23.23.23.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 34.34.34..0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] fast-reroute lfa
[PE2-ospf-1] quit
```

Configure P 2.

```
[P2] ospf
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 14.14.14.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 34.34.34.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

On P 2, set the OSPF cost to 10 for VLAN-interface 14 and VLAN-interface 34. This setting ensures that the backup LSP has a larger OSPF cost than the primary LSP.

```
[P2] interface vlan-interface 14
[P2-Vlan-interface14] ospf cost 10
[P2-Vlan-interface14] quit
[P2] interface vlan-interface 34
[P2-Vlan-interface34] ospf cost 10
[P2-Vlan-interface34] quit
```

3. Configure basic MPLS and MPLS LDP:

Configure PE 1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
[PE1] interface vlan-interface 14
[PE1-Vlan-interface14] mpls enable
[PE1-Vlan-interface14] mpls ldp enable
[PE1-Vlan-interface14] quit
```

Configure P 1.

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls ldp
[P1-ldp] quit
[P1] interface vlan-interface 12
[P1-Vlan-interface12] mpls enable
[P1-Vlan-interface12] mpls ldp enable
[P1-Vlan-interface12] quit
[P1] interface vlan-interface 23
[P1-Vlan-interface23] mpls enable
[P1-Vlan-interface23] mpls ldp enable
[P1-Vlan-interface23] quit
```

Configure PE 2.

```
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface vlan-interface 23
[PE2-Vlan-interface23] mpls enable
[PE2-Vlan-interface23] mpls ldp enable
[PE2-Vlan-interface23] quit
[PE2] interface vlan-interface 34
[PE2-Vlan-interface34] mpls enable
[PE2-Vlan-interface34] mpls ldp enable
[PE2-Vlan-interface34] quit
```

Configure P 2.

```
[P2] mpls lsr-id 4.4.4.4
[P2] mpls ldp
[P2-ldp] quit
[P2] interface vlan-interface 14
[P2-Vlan-interface14] mpls enable
[P2-Vlan-interface14] mpls ldp enable
[P2-Vlan-interface14] quit
[P2] interface vlan-interface 34
[P2-Vlan-interface34] mpls enable
[P2-Vlan-interface34] mpls ldp enable
[P2-Vlan-interface34] quit
```

Verify that LDP sessions in **Operational** state have been established on each device. The following shows the output on PE 1.

```
[PE1] display mpls ldp peer
Total number of peers: 2
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.2:0               Operational   Passive  Off  Off  55/55
4.4.4.4:0               Operational   Passive  Off  Off  6/6
```

4. Configure LSP generation policies to establish LSPs to destinations 192.168.10.0/24, 192.168.20.0/24, 1.1.1.1/32, and 3.3.3.3/32:

On PE 1, create IP prefix list **PE1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE1] ip prefix-list PE1 index 10 permit 192.168.10.0 24
[PE1] ip prefix-list PE1 index 20 permit 192.168.20.0 24
[PE1] ip prefix-list PE1 index 30 permit 1.1.1.1 32
[PE1] ip prefix-list PE1 index 40 permit 3.3.3.3 32
[PE1] mpls ldp
[PE1-ldp] lsp-trigger prefix-list PE1
[PE1-ldp] quit
```

On P 1, create IP prefix list **P1**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P1] ip prefix-list P1 index 10 permit 192.168.10.0 24
[P1] ip prefix-list P1 index 20 permit 192.168.20.0 24
[P1] ip prefix-list P1 index 30 permit 1.1.1.1 32
[P1] ip prefix-list P1 index 40 permit 3.3.3.3 32
[P1] mpls ldp
[P1-ldp] lsp-trigger prefix-list P1
[P1-ldp] quit
```

On PE 2, create IP prefix list **PE2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[PE2] ip prefix-list PE2 index 10 permit 192.168.10.0 24
[PE2] ip prefix-list PE2 index 20 permit 192.168.20.0 24
[PE2] ip prefix-list PE2 index 30 permit 1.1.1.1 32
[PE2] ip prefix-list PE2 index 40 permit 3.3.3.3 32
[PE2] mpls ldp
[PE2-ldp] lsp-trigger prefix-list PE2
[PE2-ldp] quit
```

On P 2, create IP prefix list **P2**, and configure LDP to use only the routes permitted by the prefix list to establish LSPs.

```
[P2] ip prefix-list P2 index 10 permit 192.168.10.0 24
[P2] ip prefix-list P2 index 20 permit 192.168.20.0 24
[P2] ip prefix-list P2 index 30 permit 1.1.1.1 32
[P2] ip prefix-list P2 index 40 permit 3.3.3.3 32
[P2] mpls ldp
[P2-ldp] lsp-trigger prefix-list P2
[P2-ldp] quit
```

Verify that LSPs to destination 192.168.20.0/24 have been established on PE 1. The primary LSP uses VLAN-interface 12 as the outgoing interface and the backup LSP uses VLAN-interface 14 as the outgoing interface.

```
[PE1]display mpls ldp lsp
```

```
Status Flags: * - stale, L - liberal, B - backup
Statistics:
  FECs: 4      Ingress LSPs: 4     Transit LSPs: 4     Egress LSPs: 2

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.1/32         3/-
                   -/1151(L)
                   -/1279(L)
3.3.3.3/32         -/1150              12.12.12.2      Vlan12
                   1150/1150           12.12.12.2      Vlan12
                   -/1150(B)           12.12.12.2      Vlan14
                   1150/1150(B)        12.12.12.2      Vlan14
192.168.10.0/24    1141/-
                   -/1141(L)
                   -/1141(L)
192.168.20.0/24    -/1133              12.12.12.2      Vlan12
                   1133/1133           12.12.12.2      Vlan12
                   -/1133(B)           14.14.14.4      Vlan14
                   1133/1133(B)        14.14.14.4      Vlan14
```

5. Enable BFD for MPLS and use SBFD to verify LSP connectivity:

Configure PE 1.

```
[PE1] mpls bfd enable
[PE1] sbfd local-discriminator 3000000
[PE1] mpls sbfd 3.3.3.3 32 remote 2000000
```

Configure PE 2.

```
[PE2] mpls bfd enable
[PE2] sbfd local-discriminator 2000000
[PE2] mpls sbfd 1.1.1.1 32 remote 3000000
```

Verifying the configuration

1. Display SBFD information for LSPs on PE 1 and PE 2. The following shows the output on PE 1.

```
[PE1] display mpls sbfd
 Total number of sessions: 1, 1 up, 0 down, 0 init

 FEC Type: LSP
 FEC Info:
   Destination: 3.3.3.3
   Mask Length: 32
 NHLFE ID: 2
 Local Discr: 513                  Remote Discr: 2000000
 Source IP: 1.1.1.1                Destination IP: 127.0.0.1
 Session State: Up
 Template Name: -
```

2. Execute the **`tracert mpls ipv4`** command on PE 1. The output shows that the primary LSP is in use.

NOTE:

Before you use the tracert feature, enable sending ICMP time exceeded messages on intermediate devices, and enable sending ICMP destination unreachable messages on the destination device.

```
[PE1] tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   12.12.12.2/[1148]
  1     12.12.12.2         2 ms    Transit   23.23.23.3/[1148]
  2     23.23.23.3         2 ms    Egress
```

3. Verify that the ping operation from PE 1 to PE 2 will not fail after VLAN-interface 23 on P 1 is shut down during the ping operation:

Ping PE 2 from PE 1.

```
[PE1] ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
…
```

Shut down VLAN-interface 23 on P 1.

```
[P1] interface vlan-interface 23
[P1-Vlan-interface23] shutdown
```

View the **ping** command output. The output shows that the communication was interrupted, and then immediately resumed.

```
[PE1] ping -c 100000 -a 192.168.10.1 192.168.20.1
Ping 192.168.20.1 (192.168.20.1) from 192.168.10.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.20.1: icmp_seq=0 ttl=254 time=2.576 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=254 time=1.996 ms
…
56 bytes from 192.168.20.1: icmp_seq=7 ttl=254 time=2.214 ms
Request time out
56 bytes from 192.168.20.1: icmp_seq=9 ttl=254 time=2.659 ms
56 bytes from 192.168.20.1: icmp_seq=10 ttl=254 time=5.049 ms
56 bytes from 192.168.20.1: icmp_seq=11 ttl=254 time=2.098 ms
56 bytes from 192.168.20.1: icmp_seq=12 ttl=254 time=2.225 ms
56 bytes from 192.168.20.1: icmp_seq=13 ttl=254 time=2.187 ms

--- Ping statistics for 192.168.20.1 ---
14 packet(s) transmitted, 13 packet(s) received, 7.1% packet loss
round-trip min/avg/max/std-dev = 1.990/2.455/5.049/0.772 ms
```

4. Execute the **tracert mpls ipv4** command on PE 1. The output shows that the backup LSP is in use.

```
[PE1] tracert mpls -a 192.168.10.1 ipv4 192.168.20.0 24
MPLS trace route FEC 192.168.20.0/24
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   14.14.14.4/[1276]
  1     14.14.14.4         2 ms    Transit   34.34.34.3/[1148]
```

```
  2     34.34.34.3         2 ms    Egress
```

Configuration files

- PE 1:

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
#
 mpls lsr-id 1.1.1.1
#
vlan 10
#
vlan 12
#
vlan 14
#
mpls ldp
 lsp-trigger prefix-list PE1
#
 mpls bfd enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface14
 ip address 14.14.14.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 14
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
 ip prefix-list PE1 index 10 permit 192.168.10.0 24
 ip prefix-list PE1 index 20 permit 192.168.20.0 24
 ip prefix-list PE1 index 30 permit 1.1.1.1 32
 ip prefix-list PE1 index 40 permit 3.3.3.3 32
#
 mpls sbfd 3.3.3.3 32 remote 2000000
#
```

- PE 2:

```
#
ospf 1
 fast-reroute lfa
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
vlan 23
#
vlan 30
#
vlan 34
#
 sbfd local-discriminator 2000000
#
 mpls lsr-id 3.3.3.3
#
mpls ldp
 lsp-trigger prefix-list PE2
#
 mpls bfd enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface30
```

```
 ip address 192.168.20.1 255.255.255.0
#
interface Vlan-interface34
 ip address 34.34.34.3 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 34
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 23
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
 ip prefix-list PE2 index 10 permit 192.168.10.0 24
 ip prefix-list PE2 index 20 permit 192.168.20.0 24
 ip prefix-list PE2 index 30 permit 1.1.1.1 32
 ip prefix-list PE2 index 40 permit 3.3.3.3 32
#
 mpls bfd 1.1.1.1 32
#
```

- P 1:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
vlan 12
#
vlan 23
#
mpls ldp
 lsp-trigger prefix-list P1
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
```

```
 mpls enable
 mpls ldp enable
#
interface Vlan-interface23
 ip address 23.23.23.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 23
#
 ip prefix-list P1 index 10 permit 192.168.10.0 24
 ip prefix-list P1 index 20 permit 192.168.20.0 24
 ip prefix-list P1 index 30 permit 1.1.1.1 32
 ip prefix-list P1 index 40 permit 3.3.3.3 32
#
```

- P 2:

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
#
 mpls lsr-id 4.4.4.4
#
vlan 14
#
vlan 34
#
mpls ldp
 lsp-trigger prefix-list P2
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface14
 ip address 14.14.14.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface Vlan-interface34
```

```
 ip address 34.34.34.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 34
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 14
#
 ip prefix-list P2 index 10 permit 192.168.10.0 24
 ip prefix-list P2 index 20 permit 192.168.20.0 24
 ip prefix-list P2 index 30 permit 1.1.1.1 32
 ip prefix-list P2 index 40 permit 3.3.3.3 32
#
```

Contents

Introduction

This document provides examples for configuring EVPN-DCI over an MPLS L3VPN network.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MPLS L3VPN and EVPN.

General restrictions and guidelines

Before you configure EVPN on a device, you must perform the following tasks:

1. Set the system operating mode to VXLAN mode by using the **`switch-mode`** command in system view.
2. Save the running configuration.
3. Reboot the device.

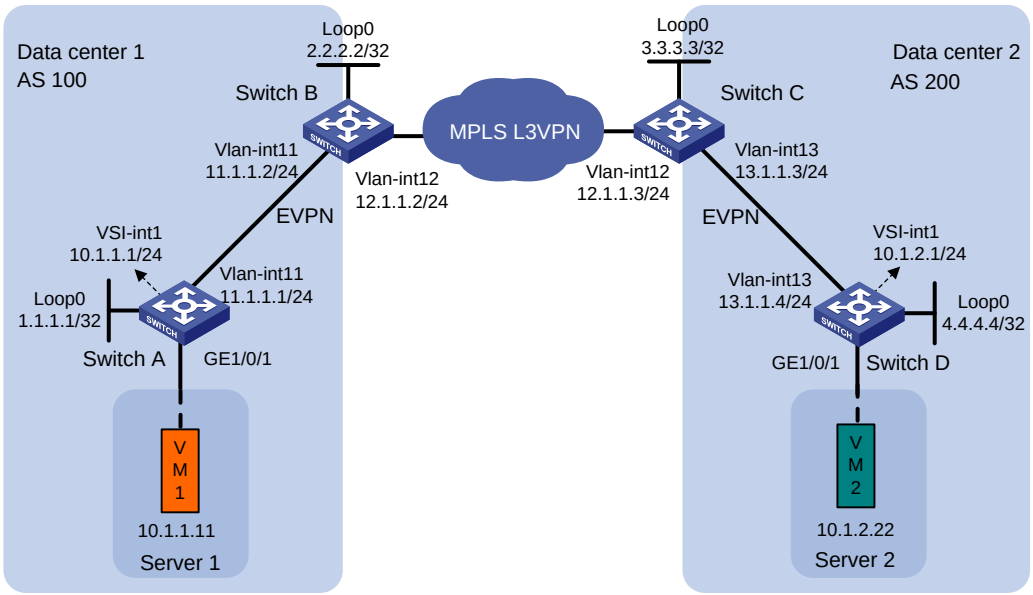
Example: Configuring IPv4 EVPN-DCI over an MPLS L3VPN network

Network configuration

As shown in Figure 1:

- Data center 1 and data center 2 are interconnected through an MPLS L3VPN network. The two data centers can communicate with each other through the MPLS L3VPN network.
- Switch A and Switch D are distributed EVPN gateways in the data centers.
- Switch B and Switch C act as both EVPN EDs and MPLS L3VPN PEs.

Figure 1 Network diagram



Analysis

For the switches within a data center to reach each other, configure a routing protocol on the switches to advertise routes for interfaces (including the loopback interfaces). In this example, OSPF is used.

To enable communication between the data centers, you must perform the following tasks on Switch B and Switch C:

- Configure both MPLS L3VPN and EVPN.
- Configure the BGP EVPN address family and the BGP VPNv4 address family to exchange routes.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-30F switch	Release 65xx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported

Hardware	Software version
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

As a best practice to ensure correct traffic forwarding, configure the same MAC address for all VSI interfaces on an EVPN gateway.

When you configure L3 VXLAN IDs for VSI interfaces, make sure the same route targets are configured for the VPN instances associated with these VSI interfaces.

Procedures

Configuring the system operating mode

Set the system operating mode to VXLAN on Switch A, and reboot the switch for the mode change to take effect.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
[SwitchA] quit
<SwitchA> reboot
```

Set the system operating mode of Switch B, Switch C, and Switch D to VXLAN. The method is the same as Switch A. (Details not shown.)

Configuring IP addresses for interfaces

Configure IP addresses for interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 11
[SwitchA-vlan11] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 11
[SwitchA-GigabitEthernet1/0/2] undo shutdown
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] undo shutdown
[SwitchA-Vlan-interface11] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] undo shutdown
[SwitchA-LoopBack0] quit
```

Configure IP addresses for interfaces on Switch B, Switch C, and Switch D. The method is the same as Switch A. (Details not shown.)

Configuring OSPF on the switches

On Switch A, specify interfaces attached to the specified network to run OSPF.

```
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

On Switch B, specify interfaces attached to the specified network to run OSPF.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

On Switch C, specify interfaces attached to the specified network to run OSPF.

```
<SwitchC> system-view
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route bgp
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
```

```
[SwitchC-ospf-1] quit
```

On Switch D, specify interfaces attached to the specified network to run OSPF.

```
<SwitchD> system-view
[SwitchD] ospf 1
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Creating the VXLANs and EVPN instances

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Create VSI **vpn1** and VXLAN 10.

```
[SwitchA] vsi vpn1
[SwitchA-vsi-vpn1] vxlan 10
[SwitchA-vsi-vpn1-vxlan-10] quit
```

Create an EVPN instance on VSI **vpn1**. Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpn1] evpn encapsulation vxlan
[SwitchA-vsi-vpn1-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpn1-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpn1-evpn-vxlan] quit
[SwitchA-vsi-vpn1] quit
```

Configuring Switch D

Enable L2VPN.

```
[SwitchD] l2vpn enable
```

Create VSI **vpn1** and VXLAN 20.

```
[SwitchD] vsi vpn1
[SwitchD-vsi-vpn1] vxlan 20
[SwitchD-vsi-vpn1-vxlan-20] quit
```

Create an EVPN instance on VSI **vpn1**. Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchD-vsi-vpn1] evpn encapsulation vxlan
[SwitchD-vsi-vpn1-evpn-vxlan] route-distinguisher auto
[SwitchD-vsi-vpn1-evpn-vxlan] vpn-target auto
[SwitchD-vsi-vpn1-evpn-vxlan] quit
[SwitchD-vsi-vpn1] quit
```

Configuring L3 VXLAN IDs and VSI interfaces

Configuring Switch A

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchA] ip vpn-instance vpna
```

```
[SwitchA-vpn-instance-vpna] route-distinguisher 1:1
[SwitchA-vpn-instance-vpna] address-family ipv4
[SwitchA-vpn-ipv4-vpna] vpn-target 2:2
[SwitchA-vpn-ipv4-vpna] quit
[SwitchA-vpn-instance-vpna] address-family evpn
[SwitchA-vpn-evpn-vpna] vpn-target 1:1
[SwitchA-vpn-evpn-vpna] quit
[SwitchA-vpn-instance-vpna] quit
```

Enable Layer 3 forwarding for VXLANs.

```
[SwitchA] vxlan ip-forwarding
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchA] interface vsi-interface 1
[SwitchA-Vsi-interface1] ip binding vpn-instance vpna
[SwitchA-Vsi-interface1] ip address 10.1.1.1 24
[SwitchA-Vsi-interface1] mac-address 1-1-1
[SwitchA-Vsi-interface1] distributed-gateway local
[SwitchA-Vsi-interface1] local-proxy-arp enable
[SwitchA-Vsi-interface1] quit
```

Create VSI-interface 2. Associate VSI-interface 2 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchA] interface vsi-interface 2
[SwitchA-Vsi-interface2] ip binding vpn-instance vpna
[SwitchA-Vsi-interface2] l3-vni 1000
[SwitchA-Vsi-interface2] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpn1**.

```
[SwitchA] vsi vpn1
[SwitchA-vsi-vpn1] gateway vsi-interface 1
[SwitchA-vsi-vpn1] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchB] ip vpn-instance vpna
[SwitchB-vpn-instance-vpna] route-distinguisher 1:2
[SwitchB-vpn-instance-vpna] address-family ipv4
[SwitchB-vpn-ipv4-vpna] vpn-target 2:2
[SwitchB-vpn-ipv4-vpna] quit
[SwitchB-vpn-instance-vpna] address-family evpn
[SwitchB-vpn-evpn-vpna] vpn-target 1:1
[SwitchB-vpn-evpn-vpna] quit
[SwitchB-vpn-instance-vpna] quit
```

Enable Layer 3 forwarding for VXLANs.

```
[SwitchB] vxlan ip-forwarding
```

Create VSI-interface 1. Associate VSI-interface 1 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchB] interface vsi-interface 1
```

```
[SwitchB-Vsi-interface1] ip binding vpn-instance vpna
[SwitchB-Vsi-interface1] l3-vni 1000
[SwitchB-Vsi-interface1] quit
```

Configuring Switch C

Enable L2VPN.

```
[SwitchC] l2vpn enable
```

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchC] ip vpn-instance vpna
[SwitchC-vpn-instance-vpna] route-distinguisher 1:3
[SwitchC-vpn-instance-vpna] address-family ipv4
[SwitchC-vpn-ipv4-vpna] vpn-target 2:2
[SwitchC-vpn-ipv4-vpna] quit
[SwitchC-vpn-instance-vpna] address-family evpn
[SwitchC-vpn-evpn-vpna] vpn-target 1:1
[SwitchC-vpn-evpn-vpna] quit
[SwitchC-vpn-instance-vpna] quit
```

Enable Layer 3 forwarding for VXLANs.

```
[SwitchC] vxlan ip-forwarding
```

Create VSI-interface 1. Associate VSI-interface 1 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchC] interface vsi-interface 1
[SwitchC-Vsi-interface1] ip binding vpn-instance vpna
[SwitchC-Vsi-interface1] l3-vni 1000
[SwitchC-Vsi-interface1] quit
```

Configuring Switch D

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchD] ip vpn-instance vpna
[SwitchD-vpn-instance-vpna] route-distinguisher 1:4
[SwitchD-vpn-instance-vpna] address-family ipv4
[SwitchD-vpn-ipv4-vpna] vpn-target 2:2
[SwitchD-vpn-ipv4-vpna] quit
[SwitchD-vpn-instance-vpna] address-family evpn
[SwitchD-vpn-evpn-vpna] vpn-target 1:1
[SwitchD-vpn-evpn-vpna] quit
[SwitchD-vpn-instance-vpna] quit
```

Enable Layer 3 forwarding for VXLANs.

```
[SwitchD] vxlan ip-forwarding
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchD] interface vsi-interface 1
[SwitchD-Vsi-interface1] ip binding vpn-instance vpna
[SwitchD-Vsi-interface1] ip address 10.1.2.1 24
[SwitchD-Vsi-interface1] mac-address 1-2-1
[SwitchD-Vsi-interface1] distributed-gateway local
[SwitchD-Vsi-interface1] local-proxy-arp enable
[SwitchD-Vsi-interface1] quit
```

Create VSI-interface 2. Associate VSI-interface 2 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchD] interface vsi-interface 2
[SwitchD-Vsi-interface2] ip binding vpn-instance vpna
[SwitchD-Vsi-interface2] l3-vni 1000
[SwitchD-Vsi-interface2] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpn1**.

```
[SwitchD] vsi vpn1
[SwitchD-vsi-vpn1] gateway vsi-interface 1
[SwitchD-vsi-vpn1] quit
```

Disabling remote MAC address learning and remote ARP learning

On Switch A, disable remote MAC address learning and remote ARP learning.

```
[SwitchA] vxlan tunnel mac-learning disable
[SwitchA] vxlan tunnel arp-learning disable
```

Disable remote MAC address learning and remote ARP learning on Switch B, Switch C, and Switch D. The method is the same as Switch A. (Details not shown.)

Mapping Ethernet service instances to VSIs

On Switch A, create Ethernet service instance 1000 on GigabitEthernet 1/0/1 to match VLAN 100 and map the Ethernet service instance to VSI **vpn1**.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] service-instance 1000
[SwitchA-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[SwitchA-GigabitEthernet1/0/1-srv1000] xconnect vsi vpn1
[SwitchA-GigabitEthernet1/0/1-srv1000] quit
[SwitchA-GigabitEthernet1/0/1] quit
```

On Switch D, create Ethernet service instance 1000 on GigabitEthernet 1/0/1 to match VLAN 100 and map the Ethernet service instance to VSI **vpn1**.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] service-instance 1000
[SwitchD-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[SwitchD-GigabitEthernet1/0/1-srv1000] xconnect vsi vpn1
[SwitchD-GigabitEthernet1/0/1-srv1000] quit
[SwitchD-GigabitEthernet1/0/1] quit
```

Establishing BGP EVPN peer relationship within a data center

Data center 1

Configure Switch A to advertise BGP EVPN routes.

```
[SwitchA] bgp 100
[SwitchA-bgp-default] peer 2.2.2.2 as-number 100
[SwitchA-bgp-default] peer 2.2.2.2 connect-interface loopback 0
```

```
[SwitchA-bgp-default] address-family l2vpn evpn
[SwitchA-bgp-default-evpn] peer 2.2.2.2 enable
[SwitchA-bgp-default-evpn] quit
[SwitchA-bgp-default] quit
```

Configure Switch B to advertise BGP EVPN routes.

```
[SwitchB] bgp 100
[SwitchB-bgp-default] peer 1.1.1.1 as-number 100
[SwitchB-bgp-default] peer 1.1.1.1 connect-interface loopback 0
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] peer 1.1.1.1 enable
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] quit
```

Data center 2

Configure Switch C to advertise BGP EVPN routes.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] peer 4.4.4.4 as-number 200
[SwitchC-bgp-default] peer 4.4.4.4 connect-interface loopback 0
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] peer 4.4.4.4 enable
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] quit
```

Configure Switch D to advertise BGP EVPN routes.

```
[SwitchD] bgp 200
[SwitchD-bgp-default] peer 3.3.3.3 as-number 200
[SwitchD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchD-bgp-default] address-family l2vpn evpn
[SwitchD-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchD-bgp-default-evpn] quit
[SwitchD-bgp-default] quit
```

Establishing MPLS L3VPN connections between ASs

Configuring Switch B

Configure the LSR ID as 2.2.2.2 for the local node, enable LDP globally, and enable MPLS and IPv4 LDP on VLAN-interface 12.

```
[SwitchB] mpls lsr-id 2.2.2.2
[SwitchB] mpls ldp
[SwitchB-ldp] quit
[SwitchB] interface vlan-interface 12
[SwitchB–Vlan-interface12] mpls enable
[SwitchB–Vlan-interface12] mpls ldp enable
[SwitchB–Vlan-interface12] quit
```

Configure BGP to advertise VPNv4 routes.

```
[SwitchB] bgp 100
[SwitchB-bgp-default] peer 12.1.1.3 as-number 200
[SwitchB-bgp-default] address-family vpnv4
[SwitchB-bgp-default-vpnv4] peer 12.1.1.3 enable
```

```
[SwitchB-bgp-default-vpnv4] quit
[SwitchB-bgp-default] quit
```

Configuring Switch C

Configure the LSR ID as 3.3.3.3 for the local node, enable LDP globally, and enable MPLS and IPv4 LDP on VLAN-interface 12.

```
[SwitchC] mpls lsr-id 3.3.3.3
[SwitchC] mpls ldp
[SwitchC -ldp] quit
[SwitchC] interface vlan-interface 12
[SwitchC–Vlan-interface12] mpls enable
[SwitchC–Vlan-interface12] mpls ldp enable
[SwitchC–Vlan-interface12] quit
```

Configure BGP to advertise VPNv4 routes.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] peer 12.1.1.2 as-number 100
[SwitchC-bgp-default] address-family vpnv4
[SwitchC-bgp-default-vpnv4] peer 12.1.1.2 enable
[SwitchC-bgp-default-vpnv4] quit
[SwitchC-bgp-default] quit
```

Configuring the BGP EVPN address family and the BGP VPNv4 address family to exchange routes

On Switch B, configure the BGP EVPN address family and the BGP VPNv4 address family to exchange routes.

```
[SwitchB] bgp 100
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] advertise l3vpn route
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] address-family vpnv4
[SwitchB-bgp-default-vpnv4] advertise evpn route
[SwitchB-bgp-default-vpnv4] quit
[SwitchB-bgp-default] quit
```

On Switch C, configure the BGP EVPN address family and the BGP VPNv4 address family to exchange routes.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] advertise l3vpn route
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] address-family vpnv4
[SwitchC-bgp-default-vpnv4] advertise evpn route
[SwitchC-bgp-default-vpnv4] quit
[SwitchC-bgp-default] quit
```

Verifying the configuration

On Switch B, display the BGP VPNv4 routing table. Verify that BGP EVPN routes are redistributed to the routing table.

```
[SwitchB] display bgp routing-table vpnv4

 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PEs: 1

 Route distinguisher: 1:2(vpna)
 Total number of routes: 3

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >i 10.1.1.0/24        1.1.1.1         0          100        0       i
* >i 10.1.1.11/32       1.1.1.1         0          100        0       i
* >e 10.1.2.0/24        12.1.1.3                               0       200i

 Route distinguisher: 1:3
 Total number of routes: 1

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >e 10.1.2.0/24        12.1.1.3                               0       200i
```

Display BGP VPNv4 route advertisement information. Verify that the BGP EVPN routes are advertised to the BGP VPNv4 neighbor.

```
[SwitchB] display bgp routing-table vpnv4 10.1.1.0 advertise-info

 BGP local router ID: 2.2.2.2
 Local AS number: 100



 Route distinguisher: 1:2
 Total number of routes: 1
 Paths:   1 best

 BGP routing table information of 10.1.1.0/24(TxPathID:0):
 Advertised to VPN peers (1 in total):
    12.1.1.3
 Inlabel              : 1150
```

Display BGP EVPN routes. Verify that an IP prefix advertisement route is generated based on the route that is redistributed in to the BGP EVPN address family from the BGP VPNv4 address family.

```
[SwitchB] display bgp l2vpn evpn
```

```
 BGP local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PEs: 2

 Route distinguisher: 1:1
 Total number of routes: 1

*>  Network : [5][0][24][10.1.1.0]/80
    NextHop : 1.1.1.1                           LocPrf    :100
    PrefVal : 0                                 OutLabel  : NULL
    MED     : 0
    Path/Ogn: i

 Route distinguisher: 1:2(vpna)
 Total number of routes: 2

*>i Network : [2][0][48][0005-0005-0005][32][10.1.1.11]/136
    NextHop : 1.1.1.1                           LocPrf    : 100
    PrefVal : 0                                 OutLabel  : NULL
    MED     : 0
    Path/Ogn: i

*>e Network : [5][0][24][10.1.2.0]/80
    NextHop : 127.0.0.1                         LocPrf    : 0
    PrefVal : 0                                 OutLabel  : NULL
    MED     : 0
    Path/Ogn: 200i

 Route distinguisher: 1:10
 Total number of routes: 1

*>i Network : [2][0][48][0005-0005-0005][32][10.1.1.11]/136
    NextHop : 1.1.1.1                           LocPrf    :100
    PrefVal : 0                                 OutLabel  : NULL
    MED     : 0
    Path/Ogn: i
```

Display detailed advertisement information about the IP prefix advertisement route. Verify that the switch has advertised the route to the EVPN neighbor.

```
[SwitchB] display bgp l2vpn evpn [5][0][24][10.1.2.0]/80 advertise-info

 BGP local router ID: 2.2.2.2
 Local AS number: 100
```

```
Route distinguisher: 1:2
Total number of routes: 1
Paths:   1 best

BGP routing table information of [5][0][24][10.1.2.0]/80(TxPathID:0):
Advertised to peers (1 in total):
    1.1.1.1
```

Configuration files

- Switch A:

```
#
 sysname SwitchA
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 11
#
vlan 100
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vpn1
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
```

```
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi vpn1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 2.2.2.2 enable
#
return
```

- Switch B:

```
#
 sysname SwitchB
#
ip vpn-instance vpna
 route-distinguisher 1:2
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
```

```
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
 mpls lsr-id 2.2.2.2
#
vlan 11 to 12
#
mpls ldp
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.2 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 12
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 100
 peer 1.1.1.1 as-number 100
```

```
 peer 1.1.1.1 connect-interface LoopBack0
 peer 12.1.1.3 as-number 200
 #
 address-family vpnv4
  advertise evpn route
  peer 12.1.1.3 enable
 #
 address-family l2vpn evpn
  advertise l3vpn route
  peer 1.1.1.1 enable
#
```

- Switch C:

```
#
 sysname SwitchC
#
ip vpn-instance vpna
 route-distinguisher 1:3
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
 mpls lsr-id 3.3.3.3
#
vlan 12 to 13
#
mpls ldp
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface12
 ip address 12.1.1.3 255.255.255.0
```

```
 mpls enable
 mpls ldp enable
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 12
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 13
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 200
 peer 4.4.4.4 as-number 200
 peer 4.4.4.4 connect-interface LoopBack0
 peer 12.1.1.2 as-number 100
 #
 address-family vpnv4
  advertise evpn route
  peer 12.1.1.2 enable
 #
 address-family l2vpn evpn
  advertise l3vpn route
  peer 4.4.4.4 enable
#
```

- Switch D:

```
#
 sysname SwitchD
#
ip vpn-instance vpna
 route-distinguisher 1:4
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
```

```
 vxlan tunnel mac-learning disable
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
vlan 13
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vpn1
 gateway vsi-interface 1
 vxlan 20
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi vpn1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 13
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.2.1 255.255.255.0
 mac-address 0001-0002-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 l3-vni 1000
```

```
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
```

Contents

Introduction

This document provides configuration examples for using Distributed Resilient Network Interconnect (DRNI) on an Ethernet Virtual Private Network (EVPN) network.

DRNI virtualizes two physical devices into one system through multichassis link aggregation. You can use DRNI to virtualize two VTEPs or EVPN gateways into one distributed-relay (DR) system to avoid single points of failure.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of DRNI and EVPN.

General restrictions and guidelines

Link aggregation group membership is mutually exclusive with Ethernet service instance-to-VSI mappings on a Layer 2 interface. Do not associate a VSI with an Ethernet service instance on a Layer 2 interface if the interface is in an aggregation group. Do not assign a Layer 2 interface to an aggregation group if the interface is configured with Ethernet service instances of VSIs.

Ethernet service instance bindings of VSIs are mutually exclusive with QinQ and VLAN mapping on a Layer 2 Ethernet interface or Layer 2 aggregate interface. Do not configure these features simultaneously on the same interface. Otherwise, the features cannot take effect.

Do not configure VLAN mapping, QinQ, or MAC-based VLAN on a Layer 2 Ethernet interface or Layer 2 aggregate interface that acts as the traffic outgoing interface of a VXLAN tunnel. Otherwise, the features cannot take effect.

If a manually created VXLAN tunnel and an automatically created VXLAN tunnel have the same destination IP address, do not assign the tunnels to the same VXLAN. For more information about manual VXLAN tunnel setup, see *VXLAN Configuration Guide*.

The VTEPs or EVPN gateways to form a DR system must have the same configuration, including the following:

- ACs.
- VSI and VXLAN mappings.
- Router MAC address, which is the EVPN global MAC address configured by using the **evpn global-mac** command or the MAC address assigned to L3VNI-associated VSI interfaces by using the **mac-address** command.

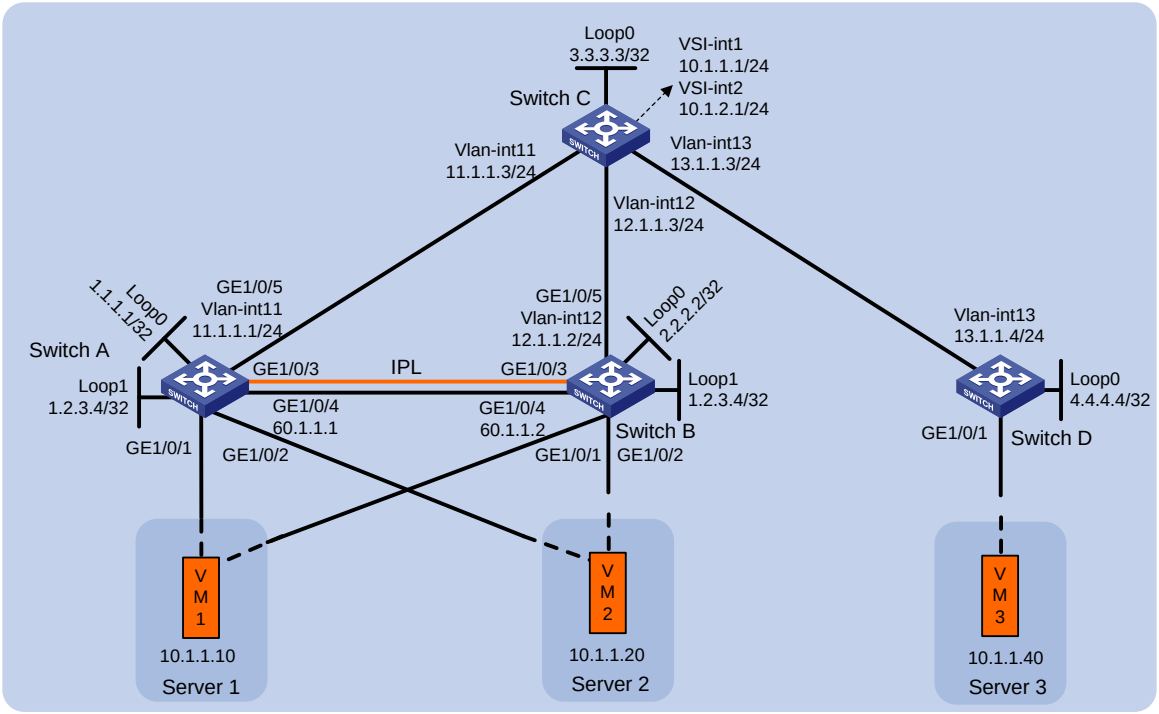
Example: Configuring DRNI using an Ethernet aggregate link as the IPL on EVPN VTEPs

Network configuration

As shown in Figure 1, perform the following tasks to make sure the VMs can communicate with one another:

- Configure VXLAN 10 on Switch A, Switch B, and Switch D.
- Configure DRNI on Switch A and Switch B to virtualize them into one VTEP. Configure an Ethernet aggregate link as the IPL between the switches.
- Configure Switch C as a route reflector (RR).

Figure 1 Network diagram



Analysis

To make sure the overlay network has connectivity, configure a routing protocol on the switches to advertise routes for reaching their interfaces, including the loopback interfaces. In this example, OSPF is used.

To conserve resources, configure Switch C to reflect routes for Switch A, Switch B, and Switch D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Make sure the following settings are consistent on the DR member devices:

- Ethernet service instances and their match criterion on the DR interfaces in the same DR group or single-homed site-facing interfaces.

- VXLAN IDs of VSIs.

In addition, the Ethernet service instances must be created manually.

As a best practice, do not redistribute external routes on the DR member devices.

Use the **drni mad exclude interface** command to exclude all interfaces used by EVPN from the shutdown action by DRNI MAD. The interfaces include VSI interfaces, interfaces that provide BGP peer addresses, interfaces used for setting up the keepalive link, and transport-facing outgoing interfaces of VXLAN tunnels.

For EVPN to run correctly on a DR system, you must execute the **undo mac-address static source-check enable** command to disable static source check on the following interfaces:

- Layer 2 aggregate interfaces or Layer 2 Ethernet interfaces acting as the IPPs.
- Transport-facing physical interfaces.

As a best practice, use the IP address of a loopback interface as the virtual VTEP address.

You must disable spanning tree on the Layer 2 Ethernet interface that acts as the physical traffic outgoing interface of a VXLAN tunnel. If you enable spanning tree on that interface, the upstream device will falsely block the interfaces connected to the DR member devices.

Configure backup routes for directing traffic from one DR member device to the other DR member device upon uplink failure.

You can configure only the **encapsulation s-vid** *vlan-id* and **encapsulation untagged** frame match criteria and VLAN access mode for Ethernet service instances

Procedures

Configuring the system operating mode

Set the system operating mode to VXLAN on Switch A, and reboot the switch for the mode change to take effect.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Set the system operating mode of Switch B and Switch D to VXLAN. The method is the same as Switch A. (Details not shown.)

Configuring routed (Layer 3) interfaces

Configure the Layer 3 interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] interface loopback 0
[SwitchA-Loopback0] ip address 1.1.1.1 32
[SwitchA-Loopback0] quit
[SwitchA] interface loopback 1
```

```
[SwitchA-Loopback1] ip address 1.2.3.4 32
[SwitchA-Loopback1] quit
[SwitchA] vlan 11
[SwitchA-vlan11] port gigabitethernet 1/0/5
[SwitchA-vlan11] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-mode route
[SwitchA-GigabitEthernet1/0/4] ip address 60.1.1.1 24
[SwitchA-GigabitEthernet1/0/4] quit
```

Configure the Layer 3 interfaces on other switches. (Details not shown.)

Configuring OSPF

Configuring Switch A

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure OSPF on VLAN-interface 100 for traffic to be redirected to an available DR member device when an uplink fails.

```
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 100.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] ospf 1 area 0.0.0.0
[SwitchA-Vlan-interface100] quit
```

Configuring Switch B

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure OSPF on VLAN-interface 100 for traffic to be redirected to an available DR member device when an uplink fails.

```
[SwitchB] vlan 100
[SwitchB-vlan100] quit
```

```
[SwitchB] interface Vlan-interface 100
[SwitchB-Vlan-interface100] ip address 100.1.1.2 255.255.255.0
[SwitchB-Vlan-interface100] ospf 1 area 0.0.0.0
[SwitchB-Vlan-interface100] quit
```

Configuring Switch C

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configuring Switch D

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Disabling spanning tree

Configuring Switch A

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/5.

```
[SwitchA] interface gigabitethernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] undo stp enable
[SwitchA-GigabitEthernet1/0/5] quit
```

Configuring Switch B

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] undo stp enable
[SwitchB-GigabitEthernet1/0/5] quit
```

Configuring EVPN

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs.

```
[SwitchA] undo vxlan ip-forwarding
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchA] vxlan tunnel mac-learning disable
[SwitchA] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] arp suppression enable
[SwitchA-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs.

```
[SwitchB] undo vxlan ip-forwarding
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchB] vxlan tunnel mac-learning disable
[SwitchB] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] arp suppression enable
[SwitchB-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
```

Configuring Switch D

Enable L2VPN.

```
[SwitchD] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs.

```
[SwitchD] undo vxlan ip-forwarding
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchD] vxlan tunnel mac-learning disable
[SwitchD] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchD] vsi vpna
[SwitchD-vsi-vpna] arp suppression enable
```

```
[SwitchD-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchD-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchD-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchD-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchD-vsi-vpna] vxlan 10
[SwitchD-vsi-vpna-vxlan-10] quit
[SwitchD-vsi-vpna] quit
```

Configuring DRNI

Configuring Switch A

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchA] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchA] drni system-mac 0001-0001-0001
[SwitchA] drni system-number 1
[SwitchA] drni system-priority 10
[SwitchA] drni restore-delay 180
[SwitchA] drni keepalive ip destination 60.1.1.2 source 60.1.1.1
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[SwitchA] interface bridge-aggregation 3
[SwitchA-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 to aggregation group 3.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchA-GigabitEthernet1/0/3] quit
```

Specify Bridge-Aggregation 3 as the IPP.

```
[SwitchA] interface bridge-aggregation 3
[SwitchA-Bridge-Aggregation3] port drni intra-portal-port 1
[SwitchA-Bridge-Aggregation3] undo mac-address static source-check enable
[SwitchA-Bridge-Aggregation3] quit
```

Disable the static source check feature on GigabitEthernet 1/0/5.

```
[SwitchA] interface gigabitethernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] undo mac-address static source-check enable
[SwitchA-GigabitEthernet1/0/5] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchA-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port drni group 4
[SwitchA-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchA-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port drni group 5
[SwitchA-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface loopback 0
[SwitchA] drni mad exclude interface gigabitethernet 1/0/4
[SwitchA] drni mad exclude interface gigabitethernet 1/0/5
[SwitchA] drni mad exclude interface vlan-interface 11
```

Configuring Switch B

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchB] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchB] drni system-mac 0001-0001-0001
[SwitchB] drni system-number 2
[SwitchB] drni system-priority 10
[SwitchB] drni restore-delay 180
[SwitchB] drni keepalive ip destination 60.1.1.1 source 60.1.1.2
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[SwitchB] interface bridge-aggregation 3
[SwitchB-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 to aggregation group 3.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchB-GigabitEthernet1/0/3] quit
```

Specify Bridge-Aggregation 3 as the IPP.

```
[SwitchB] interface bridge-aggregation 3
[SwitchB-Bridge-Aggregation3] port drni intra-portal-port 1
[SwitchB-Bridge-Aggregation3] undo mac-address static source-check enable
[SwitchB-Bridge-Aggregation3] quit
```

Disable the static source check feature on GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] undo mac-address static source-check enable
```

```
[SwitchB-GigabitEthernet1/0/5] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port drni group 4
[SwitchB-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchB-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port drni group 5
[SwitchB-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface loopback 0
[SwitchB] drni mad exclude interface gigabitethernet 1/0/4
[SwitchB] drni mad exclude interface gigabitethernet 1/0/5
[SwitchA] drni mad exclude interface vlan-interface 12
```

Configuring BGP to advertise BGP EVPN routes

Configuring Switch A

Configure BGP to advertise BGP EVPN routes.

```
[SwitchA] bgp 200
[SwitchA-bgp-default] peer 3.3.3.3 as-number 200
[SwitchA-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchA-bgp-default] address-family l2vpn evpn
[SwitchA-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchA-bgp-default-evpn] quit
[SwitchA-bgp-default] quit
```

Configuring Switch B

Configure BGP to advertise BGP EVPN routes.

```
[SwitchB] bgp 200
[SwitchB-bgp-default] peer 3.3.3.3 as-number 200
```

```
[SwitchB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] quit
```

Configuring Switch C

Configure BGP to advertise BGP EVPN routes and configure the switch as an RR.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] group evpn
[SwitchC-bgp-default] peer 1.1.1.1 group evpn
[SwitchC-bgp-default] peer 2.2.2.2 group evpn
[SwitchC-bgp-default] peer 4.4.4.4 group evpn
[SwitchC-bgp-default] peer evpn as-number 200
[SwitchC-bgp-default] peer evpn connect-interface loopback 0
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] peer evpn enable
[SwitchC-bgp-default-evpn] undo policy vpn-target
[SwitchC-bgp-default-evpn] peer evpn reflect-client
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] quit
```

Configuring Switch D

Configure BGP to advertise BGP EVPN routes.

```
[SwitchD] bgp 200
[SwitchD-bgp-default] peer 3.3.3.3 as-number 200
[SwitchD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchD-bgp-default] address-family l2vpn evpn
[SwitchD-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchD-bgp-default-evpn] quit
[SwitchD-bgp-default] quit
```

Mapping Ethernet service instances to VSIs

Configuring Switch A

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchA-Bridge-Aggregation4] service-instance 1000
[SwitchA-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port link-type trunk
[SwitchA-Bridge-Aggregation5] port trunk permit vlan 3
```

```
[SwitchA-Bridge-Aggregation5] service-instance 1000
[SwitchA-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-Bridge-Aggregation5-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch B

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port link-type trunk
[SwitchB-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchB-Bridge-Aggregation4] service-instance 1000
[SwitchB-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port link-type trunk
[SwitchB-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchB-Bridge-Aggregation5] service-instance 1000
[SwitchB-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation5-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch D

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchD-GigabitEthernet1/0/1] service-instance 1000
[SwitchD-GigabitEthernet1/0/1] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchD-GigabitEthernet1/0/1] xconnect vsi vpna
[SwitchD-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verifying the configuration on a DR member device

The verification procedure uses Switch A as an example.

Verify that Switch A has BGP EVPN routes.

```
[Switch A]display bgp l2vpn evpn
 BGP local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
```

```
              a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
 Total number of routes from all PEs: 1
 Route distinguisher: 1:10
 Total number of routes: 2
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][4.4.4.4]/80
                        4.4.4.4         0          100        0       i
```

Verify that the VXLAN tunnel to Switch D is up, and the source address of the tunnel is the virtual VTEP address.

```
[SwitchA] display interface tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.2.3.4, destination 4.4.4.4
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that ACs have been created on the IPP and mapped to VXLAN 10.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel0              0x5000000  UP       Auto        Disabled
  ACs:
```

```
AC                              Link ID  State       Type
BAGG4 srv1000                   0        Up          Manual
BAGG3 srv2                      1        Up          Dynamic (DRNI)
BAGG5 srv1000                   2        Up          Manual
BAGG3 srv3                      3        Up          Dynamic (DRNI)
```

Verifying the network connectivity of the VMs

Verify that VM 1, VM 2, and VM 3 can communicate when both Switch A and Switch B are operating correctly. (Details not shown.)

Verify that VM 1, VM 2, and VM 3 can communicate when Switch A's or Switch B's links to the local site are disconnected. (Details not shown.)

Configuration files

- Switch A:

```
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 11
#
vlan 100
#
l2vpn enable
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation3
```

```
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpna
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack0
 ip address 1.2.3.4 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 60.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-aggregation group 3
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 11
 undo stp enable
 undo mac-address static source-check enable
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni keepalive ip destination 60.1.1.2 source 60.1.1.1
 drni restore-delay 180
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/4
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface11
#
return
```

- Switch B:

```
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.1.1.0 0.0.0.255
#
vlan 2
#
```

```
vlan 3
#
vlan 12
#
vlan 100
#
l2vpn enable
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpna
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
```

```
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 60.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-aggregation group 3
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 12
 undo stp enable
 undo mac-address static source-check enable
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni keepalive ip destination 60.1.1.1 source 60.1.1.2
 drni restore-delay 180
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
```

```
 drni mad exclude interface GigabitEthernet1/0/4
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface12
#
return
```

- Switch C:

```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 11.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 11 to 13
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.3 255.255.255.0
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
bgp 200
 group evpn internal
 peer evpn connect-interface LoopBack0
 peer 1.1.1.1 group evpn
 peer 2.2.2.2 group evpn
 peer 4.4.4.4 group evpn
 #
 address-family l2vpn evpn
```

```
  undo policy vpn-target
  peer evpn enable
  peer evpn reflect-client
#
return
```

- Switch D:

```
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
vlan 2
#
vlan 13
#
l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 13
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
```

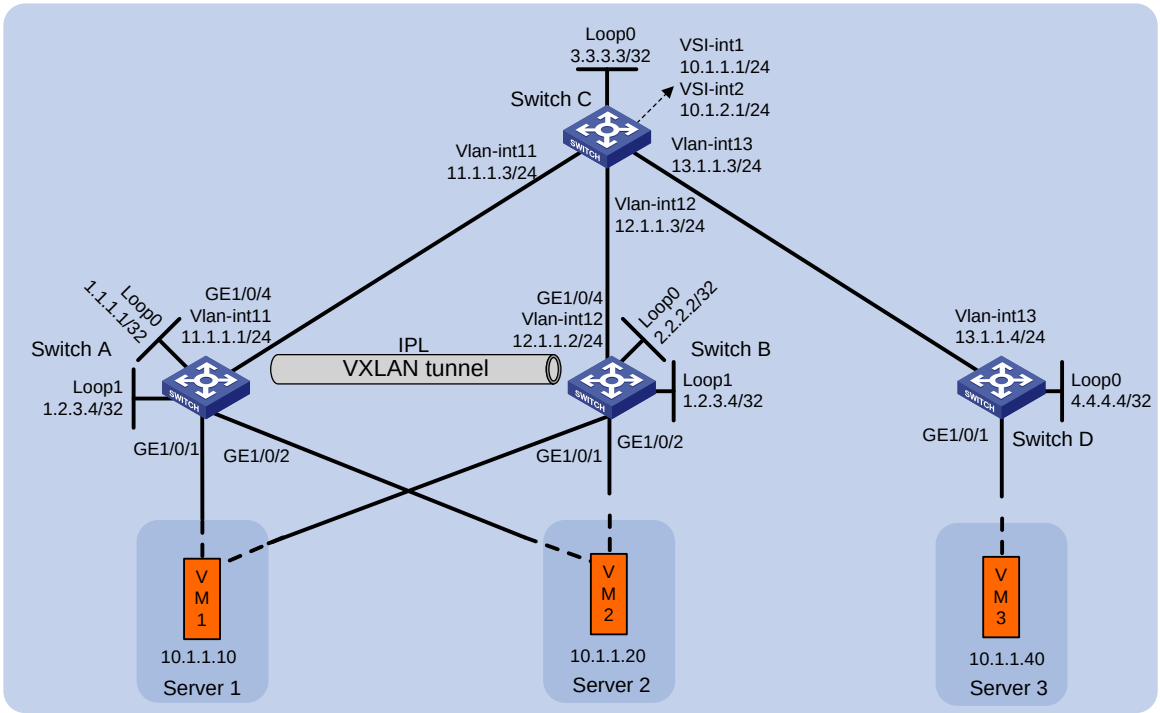
Example: Configuring DRNI using a VXLAN tunnel as the IPL on EVPN VTEPs

Network configuration

As shown in Figure 2, perform the following tasks to make sure the VMs can communicate with one another:

- Configure VXLAN 10 on Switch A, Switch B, and Switch D.
- Configure DRNI on Switch A and Switch B to virtualize them into one VTEP. Manually set up a VXLAN tunnel as the IPL between the switches.
- Configure Switch C as an RR.

Figure 2 Network diagram



Analysis

To make sure the overlay network has connectivity,, configure a routing protocol on these switches to advertise routes for reaching their interfaces, including the loopback interfaces. In this example, OSPF is used.

To conserve resources, configure Switch C to reflect routes for Switch A, Switch B, and Switch D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series	Not supported

Hardware	Software version
S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Make sure the following settings are consistent on the DR member devices:

- Ethernet service instances and their match criterion on the DR interfaces in the same DR group or single-homed site-facing interfaces.
- VXLAN IDs of VSIs.

In addition, the Ethernet service instances must be created manually.

As a best practice, do not redistribute external routes on the DR member devices.

Use the **drni mad exclude interface** command to exclude all interfaces used by EVPN from the shutdown action by DRNI MAD. The interfaces include VSI interfaces, interfaces that provide BGP peer addresses, interfaces used for setting up the keepalive link, and transport-facing outgoing interfaces of VXLAN tunnels.

Use the **drni mad exclude interface** command to exclude VXLAN tunnel interfaces and their traffic outgoing interfaces from the MAD shutdown action by DRNI before you configure them as IPPs. If you have configured the VXLAN tunnel interfaces as IPPs before excluding them and their traffic outgoing interfaces from the MAD shutdown action, you must first remove the IPP configuration. After the VXLAN tunnel interfaces and their traffic outgoing interfaces come up, exclude the interfaces from the MAD shutdown action by DRNI. Then, configure the VXLAN tunnel interfaces as IPPs.

As a best practice, use the IP address of a loopback interface as the virtual VTEP address.

For EVPN to run correctly on a DR system, you must execute the **undo mac-address static source-check enable** command to disable static source check on the following interfaces:

- Layer 2 aggregate interfaces or Layer 2 Ethernet interfaces acting as the IPPs.
- Transport-facing physical interfaces.

You must disable spanning tree on the Layer 2 Ethernet interface that acts as the physical traffic outgoing interface of a VXLAN tunnel. If you enable spanning tree on that interface, the upstream device will falsely block the interfaces connected to the DR member devices.

Procedures

Configuring the system operating mode

Set the system operating mode to VXLAN on Switch A, and reboot the switch for the mode change to take effect.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Set the system operating mode of Switch B and Switch D to VXLAN. The method is the same as Switch A. (Details not shown.)

Configuring Layer 3 interfaces

Configure the Layer 3 interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] interface loopback 0
[SwitchA-Loopback0] ip address 1.1.1.1 32
[SwitchA-Loopback0] quit
[SwitchA] interface loopback 1
[SwitchA-Loopback1] ip address 1.2.3.4 32
[SwitchA-Loopback1] quit
[SwitchA] vlan 11
[SwitchA-vlan11] port gigabitethernet 1/0/5
[SwitchA-vlan11] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] quit
```

Configure the Layer 3 interfaces on other switches. (Details not shown.)

Configuring OSPF

Configuring Switch A

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configuring Switch B

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
```

```
[SwitchC-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configuring Switch D

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Configuring EVPN

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchA] vxlan tunnel mac-learning disable
[SwitchA] vxlan tunnel arp-learning disable
```

Specify the reserved VXLAN as VXLAN 1234.

```
[SwitchA] reserved vxlan 1234
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] arp suppression enable
[SwitchA-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchB] vxlan tunnel mac-learning disable
[SwitchB] vxlan tunnel arp-learning disable
```

Specify the reserved VXLAN as VXLAN 1234.

```
[SwitchB] reserved vxlan 1234
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] arp suppression enable
[SwitchB-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
```

Configuring Switch D

Enable L2VPN.

```
[SwitchD] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchD] vxlan tunnel mac-learning disable
[SwitchD] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchD] vsi vpna
[SwitchD-vsi-vpna] arp suppression enable
[SwitchD-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchD-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchD-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchD-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchD-vsi-vpna] vxlan 10
[SwitchD-vsi-vpna-vxlan-10] quit
[SwitchD-vsi-vpna] quit
```

Configuring DRNI

Configuring Switch A

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchA] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchA] drni system-mac 0001-0001-0001
[SwitchA] drni system-number 1
[SwitchA] drni system-priority 10
[SwitchA] drni restore-delay 180
```

Create a tunnel to Switch B, and set the ToS of tunneled packets to 100.

```
[SwitchA] interface tunnel 1 mode vxlan
[SwitchA-Tunnel1] source 1.1.1.1
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] tunnel tos 100
[SwitchA-Tunnel1] quit
```

Exclude Tunnel 1 from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface tunnel 1
```

Specify Tunnel 1 as the IPP

```
[SwitchA] interface tunnel 1
[SwitchA-Tunnel1] port drni intra-portal-port 1
[SwitchA-Tunnel1] quit
```

Disable the static source check feature on GigabitEthernet 1/0/4.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] undo mac-address static source-check enable
[SwitchA-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchA-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port drni group 4
[SwitchA-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchA-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port drni group 5
[SwitchA-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface tunnel 1
[SwitchA] drni mad exclude interface loopback 0
[SwitchA] drni mad exclude interface gigabitethernet 1/0/4
[SwitchA] drni mad exclude interface vlan-interface 11
```

Configuring Switch B

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchB] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchB] drni system-mac 0001-0001-0001
[SwitchB] drni system-number 2
```

```
[SwitchB] drni system-priority 10
[SwitchB] drni restore-delay 180
```

Create a tunnel to Switch A, and set the ToS of tunneled packets to 100.

```
[SwitchB] interface tunnel 1 mode vxlan
[SwitchB-Tunnel1] source 2.2.2.2
[SwitchB-Tunnel1] destination 1.1.1.1
[SwitchB-Tunnel1] tunnel tos 100
[SwitchB-Tunnel1] quit
```

Exclude Tunnel 1 from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface tunnel 1
```

Specify Tunnel 1 as the IPP

```
[SwitchB] interface tunnel 1
[SwitchB-Tunnel1] port drni intra-portal-port 1
[SwitchB-Tunnel1] quit
```

Disable the static source check feature on GigabitEthernet 1/0/4.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] undo mac-address static source-check enable
[SwitchB-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port drni group 4
[SwitchB-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchB-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port drni group 5
[SwitchB-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface tunnel 1
[SwitchB] drni mad exclude interface loopback 0
```

```
[SwitchB] drni mad exclude interface gigabitethernet 1/0/4
[SwitchB] drni mad exclude interface vlan-interface 12
```

Configuring BGP to advertise BGP EVPN routes

Configuring Switch A

Configure BGP to advertise BGP EVPN routes.

```
[SwitchA] bgp 200
[SwitchA-bgp-default] peer 3.3.3.3 as-number 200
[SwitchA-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchA-bgp-default] address-family l2vpn evpn
[SwitchA-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchA-bgp-default-evpn] quit
[SwitchA-bgp-default] quit
```

Configuring Switch B

Configure BGP to advertise BGP EVPN routes.

```
[SwitchB] bgp 200
[SwitchB-bgp-default] peer 3.3.3.3 as-number 200
[SwitchB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] quit
```

Configuring Switch C

Configure BGP to advertise BGP EVPN routes and configure the switch as an RR.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] group evpn
[SwitchC-bgp-default] peer 1.1.1.1 group evpn
[SwitchC-bgp-default] peer 2.2.2.2 group evpn
[SwitchC-bgp-default] peer 4.4.4.4 group evpn
[SwitchC-bgp-default] peer evpn as-number 200
[SwitchC-bgp-default] peer evpn connect-interface loopback 0
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] peer evpn enable
[SwitchC-bgp-default-evpn] undo policy vpn-target
[SwitchC-bgp-default-evpn] peer evpn reflect-client
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] quit
```

Configuring Switch D

Configure BGP to advertise BGP EVPN routes.

```
[SwitchD] bgp 200
[SwitchD-bgp-default] peer 3.3.3.3 as-number 200
[SwitchD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchD-bgp-default] address-family l2vpn evpn
[SwitchD-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchD-bgp-default-evpn] quit
[SwitchD-bgp-default] quit
```

Mapping Ethernet service instances to VSIs

Configuring Switch A

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchA-Bridge-Aggregation4] service-instance 1000
[SwitchA-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna.**

```
[SwitchA-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port link-type trunk
[SwitchA-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchA-Bridge-Aggregation5] service-instance 1000
[SwitchA-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-Bridge-Aggregation5-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch B

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port link-type trunk
[SwitchB-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchB-Bridge-Aggregation4] service-instance 1000
[SwitchB-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port link-type trunk
[SwitchB-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchB-Bridge-Aggregation5] service-instance 1000
[SwitchB-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation5-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch D

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] service-instance 1000
[SwitchD-GigabitEthernet1/0/1] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchD-GigabitEthernet1/0/1] xconnect vsi vpna
[SwitchD-GigabitEthernet1/0/1] quit
```

Configuring Monitor Link

Configuring Switch A

Create monitor link group 1 and assign the uplink and downlink interfaces to it.

```
[SwitchA] monitor-link group 1
[SwitchA-mtlk-group1] port gigabitethernet 1/0/1 downlink
[SwitchA-mtlk-group1] port gigabitethernet 1/0/2 downlink
[SwitchA-mtlk-group1] port gigabitethernet 1/0/4 uplink
[SwitchA-mtlk-group1] quit
```

Configuring Switch B

Create monitor link group 1 and assign the uplink and downlink interfaces to it.

```
[SwitchB] monitor-link group 1
[SwitchB-mtlk-group1] port gigabitethernet 1/0/1 downlink
[SwitchB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[SwitchB-mtlk-group1] port gigabitethernet 1/0/4 uplink
[SwitchB-mtlk-group1] quit
```

Verifying the configuration

Verifying the configuration on a DR member device

The verification procedure uses Switch A as an example.

Verify that Switch A has BGP EVPN routes.

```
[Switch A]display bgp l2vpn evpn
 BGP local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
 Total number of routes from all PEs: 2
 Route distinguisher: 1:10
 Total number of routes: 4
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.1.1.1]/80
                        1.1.1.1         0          100        32768   i
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][2.2.2.2]/80
                        2.2.2.2         0          100        0       i
* >i [3][0][32][4.4.4.4]/80
                        4.4.4.4         0          100        0       i
```

Verify that the IPL Tunnel 1 is up, and Tunnel 0 to Switch D uses the virtual VTEP address as the source address.

```
[SwitchA] display interface Tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.2.3.4, destination 4.4.4.4
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 13 bytes/sec, 104 bits/sec, 0 packets/sec
Last 300 seconds output rate: 13 bytes/sec, 104 bits/sec, 0 packets/sec
Input: 332 packets, 36377 bytes, 0 drops
Output: 583 packets, 59132 bytes, 0 drops
```

Verify that the VXLAN tunnels have been assigned to VXLAN 10.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  VXLAN ID                : 10
  Tunnels:
```

```
  Tunnel Name          Link ID    State    Type        Flood proxy
  Tunnel0              0x5000000  UP       Auto        Disabled
  Tunnel1              0x5000001  UP       Manual      Disabled
ACs:
  AC                                Link ID  State       Type
  BAGG4 srv1000                     0        Up          Manual
  BAGG5 srv1000                     2        Up          Manual
```

Verifying the network connectivity of the VMs

Verify that VM 1, VM 2, and VM 3 can communicate when both Switch A and Switch B are operating correctly. (Details not shown.)

Verify that VM 1, VM 2, and VM 3 can communicate when Switch A's or Switch B's links to the local site are disconnected. (Details not shown.)

Configuration files

- Switch A:

```
#
monitor-link group 1
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 11
#
 l2vpn enable
 reserved vxlan 1234
 vxlan tunnel mac-learning disable
 evpn drni group 1.2.3.4
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
```

```
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpna
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 11
```

```
 undo stp enable
 port monitor-link group 1 uplink
 undo mac-address static source-check enable
#
interface Tunnel1 mode vxlan
 port drni intra-portal-port 1
 source 1.1.1.1
 destination 2.2.2.2
 tunnel tos 100
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni restore-delay 180
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Tunnel1
 drni mad exclude interface Vlan-interface 11
#
return
```

- Switch B:

```
#
monitor-link group 1
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 12
#
```

```
 l2vpn enable
 reserved vxlan 1234
 evpn drni group 1.2.3.4
 vxlan tunnel arp-learning disable
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpna
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port monitor-link group 1 downlink
 port link-aggregation group 4
```

```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port monitor-link group 1 downlink
 port link-aggregation group 5
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 12
 port monitor-link group 1 uplink
 undo mac-address static source-check enable
#
interface Tunnel1 mode vxlan
 port drni intra-portal-port 1
 source 2.2.2.2
 destination 1.1.1.1
 tunnel tos 100
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni restore-delay 180
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Tunnel1
 drni mad exclude interface Vlan-interface 12
#
return
```

- Switch C:

```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 11.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 11 to 13
```

```
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.3 255.255.255.0
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
bgp 200
 group evpn internal
 peer evpn connect-interface LoopBack0
 peer 1.1.1.1 group evpn
 peer 2.2.2.2 group evpn
 peer 4.4.4.4 group evpn
 #
 address-family l2vpn evpn
  undo policy vpn-target
  peer evpn enable
  peer evpn reflect-client
#
return
```

- Switch D:

```
#
 undo vxlan ip-forwarding
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 13.1.1.0 0.0.0.255
```

```
#
vlan 2
#
vlan 13
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vpna
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
return
```

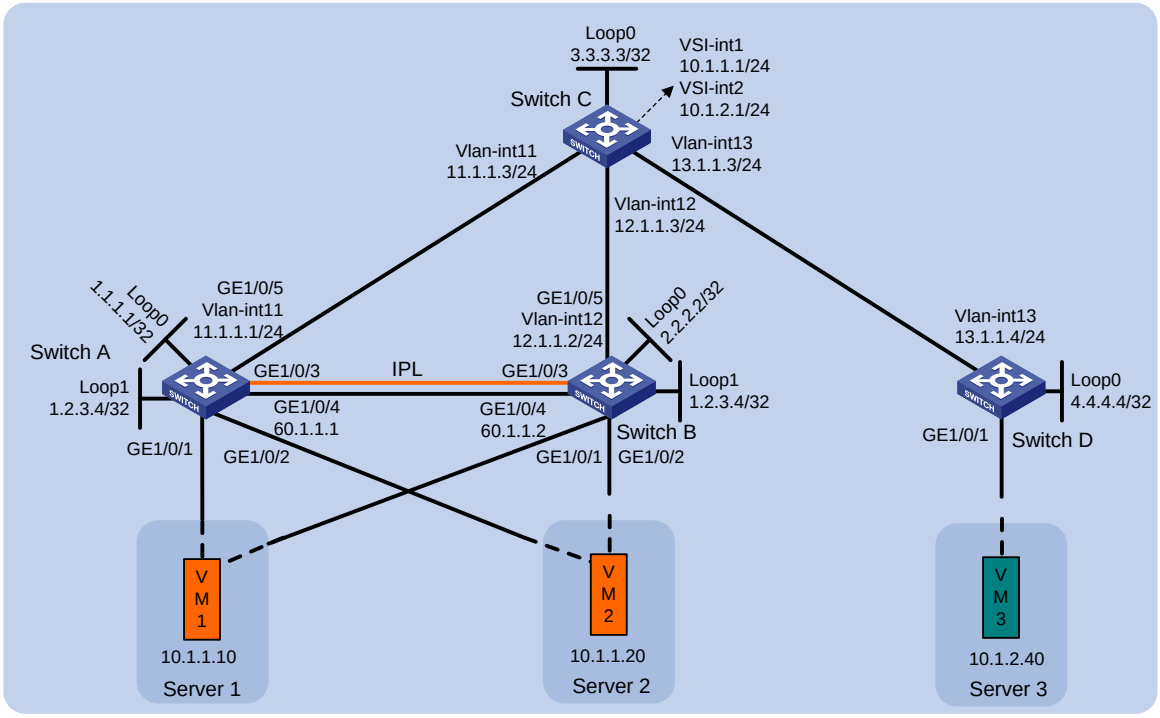
Example: Configuring DRNI using an Ethernet aggregate link as the IPL on EVPN gateways

Network configuration

As shown in Figure 3, perform the following tasks to make sure the VMs can communicate with one another:

- Configure VXLAN 10 on Switch A, Switch B, and Switch D, and configure VXLAN 20 on Switch A and Switch B.
- Configure Switch A, Switch B, and Switch D as distributed EVPN gateways to provide Layer 3 forwarding service for the VMs.
- Configure DRNI on Switch A and Switch B to virtualize them into one VTEP. Configure an Ethernet aggregate link as the IPL between the switches.
- Configure Switch C as an RR.

Figure 3 Network diagram



Analysis

To make sure the overlay network has connectivity,, configure a routing protocol on these switches to advertise routes for reaching their interfaces, including the loopback interfaces. In this example, OSPF is used.

To conserve resources, configure Switch C to reflect routes for Switch A, Switch B, and Switch D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Make sure the following settings are consistent on the DR member devices:

- Ethernet service instances and their match criterion on the DR interfaces in the same DR group or single-homed site-facing interfaces.

- VXLAN IDs of VSIs.

In addition, the Ethernet service instances must be created manually.

As a best practice, do not redistribute external routes on the DR member devices.

Use the **drni mad exclude interface** command to exclude all interfaces used by EVPN from the shutdown action by DRNI MAD. The interfaces include VSI interfaces, interfaces that provide BGP peer addresses, interfaces used for setting up the keepalive link, and transport-facing outgoing interfaces of VXLAN tunnels.

For EVPN to run correctly on a DR system, you must execute the **undo mac-address static source-check enable** command to disable static source check on the following interfaces:

- Layer 2 aggregate interfaces or Layer 2 Ethernet interfaces acting as the IPPs.
- Transport-facing physical interfaces.

As a best practice, use the IP address of a loopback interface as the virtual VTEP address.

You must disable spanning tree on the Layer 2 Ethernet interface that acts as the physical traffic outgoing interface of a VXLAN tunnel. If you enable spanning tree on that interface, the upstream device will falsely block the interfaces connected to the DR member devices.

Configure backup routes for directing traffic from one DR member device to the other DR member device upon uplink failure.

You can configure only the **encapsulation s-vid** *vlan-id* and **encapsulation untagged** frame match criteria and VLAN access mode for Ethernet service instances

Procedures

Configuring the system operating mode

Set the system operating mode to VXLAN on Switch A, and reboot the switch for the mode change to take effect.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Set the system operating mode of Switch B and Switch D to VXLAN. The method is the same as Switch A. (Details not shown.)

Configuring Layer 3 interfaces

Configure the Layer 3 interfaces on Switch A.

```
<SwitchA> system-view
[SwitchA] interface loopback 0
[SwitchA-Loopback0] ip address 1.1.1.1 32
[SwitchA-Loopback0] quit
[SwitchA] interface loopback 1
```

```
[SwitchA-Loopback1] ip address 1.2.3.4 32
[SwitchA-Loopback1] quit
[SwitchA] vlan 11
[SwitchA-vlan11] port gigabitethernet 1/0/5
[SwitchA-vlan11] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-mode route
[SwitchA-GigabitEthernet1/0/4] ip address 60.1.1.1 24
[SwitchA-GigabitEthernet1/0/4] quit
```

Configure the Layer 3 interfaces on other switches. (Details not shown.)

On VM 1, VM 3, and VM 5, specify 10.1.1.1 as the gateway address. On VM 2 and VM 4, specify 10.1.2.1 as the gateway address. (Details not shown.)

Configuring OSPF

Configuring Switch A

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure OSPF on VLAN-interface 100 for traffic to be redirected to an available DR member device when an uplink fails.

```
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 100.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] ospf 1 area 0.0.0.0
[SwitchA-Vlan-interface100] quit
```

Configuring Switch B

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure OSPF on VLAN-interface 100 for traffic to be redirected to an available DR member device when an uplink fails.

```
[SwitchB] vlan 100
[SwitchB-vlan100] quit
[SwitchB] interface Vlan-interface 100
[SwitchB-Vlan-interface100] ip address 100.1.1.2 255.255.255.0
[SwitchB-Vlan-interface100] ospf 1 area 0.0.0.0
[SwitchB-Vlan-interface100] quit
```

Configuring Switch C

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configuring Switch D

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Disabling spanning tree

Configuring Switch A

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/5.

```
[SwitchA] interface gigabitethernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] undo stp enable
[SwitchA-GigabitEthernet1/0/5] quit
```

Configuring Switch B

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] undo stp enable
[SwitchB-GigabitEthernet1/0/5] quit
```

Configuring EVPN

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchA] vxlan tunnel mac-learning disable
[SwitchA] vxlan tunnel arp-learning disable
```

Configure the EVPN global MAC address as **0002-0003-0004**.

```
[SwitchA] evpn global-mac 2-3-4
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
```

Create an EVPN instance on VSI **vpnb**.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpnb-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpnb-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpnb-evpn-vxlan] quit
```

Create VXLAN 20.

```
[SwitchA-vsi-vpnb] vxlan 20
[SwitchA-vsi-vpnb-vxlan-20] quit
[SwitchA-vsi-vpnb] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchB] vxlan tunnel mac-learning disable
[SwitchB] vxlan tunnel arp-learning disable
```

Configure the EVPN global MAC address as **0002-0003-0004**.

```
[SwitchB] evpn global-mac 2-3-4
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
```

Create an EVPN instance on VSI **vpnb**.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpnb-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpnb-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpnb-evpn-vxlan] quit
```

Create VXLAN 20.

```
[SwitchB-vsi-vpnb] vxlan 20
[SwitchB-vsi-vpnb-vxlan-20] quit
[SwitchB-vsi-vpnb] quit
```

Configuring Switch D

Enable L2VPN.

```
[SwitchD] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchD] vxlan tunnel mac-learning disable
[SwitchD] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchD] vsi vpna
[SwitchD-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchD-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchD-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchD-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchD-vsi-vpna] vxlan 10
[SwitchD-vsi-vpna-vxlan-10] quit
[SwitchD-vsi-vpna] quit
```

Configuring distributed EVPN gateways

Configuring Switch A

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchA] ip vpn-instance vpna
[SwitchA-vpn-instance-vpna] route-distinguisher 1:1
[SwitchA-vpn-instance-vpna] address-family ipv4
[SwitchA-vpn-ipv4-vpna] vpn-target 2:2
[SwitchA-vpn-ipv4-vpna] quit
[SwitchA-vpn-instance-vpna] address-family evpn
[SwitchA-vpn-evpn-vpna] vpn-target 1:1
[SwitchA-vpn-evpn-vpna] quit
[SwitchA-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchA] interface vsi-interface 1
[SwitchA-Vsi-interface1] ip binding vpn-instance vpna
[SwitchA-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
```

```
[SwitchA-Vsi-interface1] mac-address 1-1-1
[SwitchA-Vsi-interface1] distributed-gateway local
[SwitchA-Vsi-interface1] local-proxy-arp enable
[SwitchA-Vsi-interface1] quit
```

Configure VSI-interface 2 as a distributed gateway.

```
[SwitchA] interface vsi-interface 2
[SwitchA-Vsi-interface2] ip binding vpn-instance vpna
[SwitchA-Vsi-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchA-Vsi-interface2] mac-address 2-2-2
[SwitchA-Vsi-interface2] distributed-gateway local
[SwitchA-Vsi-interface2] local-proxy-arp enable
[SwitchA-Vsi-interface2] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchA] interface vsi-interface 3
[SwitchA-Vsi-interface3] ip binding vpn-instance vpna
[SwitchA-Vsi-interface3] l3-vni 1000
[SwitchA-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] gateway vsi-interface 1
[SwitchA-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for VSI **vpnb**.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] gateway vsi-interface 2
[SwitchA-vsi-vpnb] quit
```

Configuring Switch B

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchB] ip vpn-instance vpna
[SwitchB-vpn-instance-vpna] route-distinguisher 1:1
[SwitchB-vpn-instance-vpna] address-family ipv4
[SwitchB-vpn-ipv4-vpna] vpn-target 2:2
[SwitchB-vpn-ipv4-vpna] quit
[SwitchB-vpn-instance-vpna] address-family evpn
[SwitchB-vpn-evpn-vpna] vpn-target 1:1
[SwitchB-vpn-evpn-vpna] quit
[SwitchB-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchB] interface vsi-interface 1
[SwitchB-Vsi-interface1] ip binding vpn-instance vpna
[SwitchB-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[SwitchB-Vsi-interface1] mac-address 1-1-1
[SwitchB-Vsi-interface1] distributed-gateway local
[SwitchB-Vsi-interface1] local-proxy-arp enable
[SwitchB-Vsi-interface1] quit
```

Configure VSI-interface 2 as a distributed gateway.

```
[SwitchB] interface vsi-interface 2
```

```
[SwitchB-Vsi-interface2] ip binding vpn-instance vpna
[SwitchB-Vsi-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchB-Vsi-interface2] mac-address 2-2-2
[SwitchB-Vsi-interface2] distributed-gateway local
[SwitchB-Vsi-interface2] local-proxy-arp enable
[SwitchB-Vsi-interface2] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchB] interface vsi-interface 3
[SwitchB-Vsi-interface3] ip binding vpn-instance vpna
[SwitchB-Vsi-interface3] l3-vni 1000
[SwitchB-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] gateway vsi-interface 1
[SwitchB-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for VSI **vpnb**.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] gateway vsi-interface 2
[SwitchB-vsi-vpnb] quit
```

Configuring Switch D

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchD] ip vpn-instance vpna
[SwitchD-vpn-instance-vpna] route-distinguisher 1:1
[SwitchD-vpn-instance-vpna] address-family ipv4
[SwitchD-vpn-ipv4-vpna] vpn-target 2:2
[SwitchD-vpn-ipv4-vpna] quit
[SwitchD-vpn-instance-vpna] address-family evpn
[SwitchD-vpn-evpn-vpna] vpn-target 1:1
[SwitchD-vpn-evpn-vpna] quit
[SwitchD-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchD] interface vsi-interface 1
[SwitchD-Vsi-interface1] ip binding vpn-instance vpna
[SwitchD-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[SwitchD-Vsi-interface1] mac-address 1-1-1
[SwitchD-Vsi-interface1] distributed-gateway local
[SwitchD-Vsi-interface1] local-proxy-arp enable
[SwitchD-Vsi-interface1] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna** and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchD] interface vsi-interface 3
[SwitchD-Vsi-interface3] ip binding vpn-instance vpna
[SwitchD-Vsi-interface3] l3-vni 1000
[SwitchD-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchD] vsi vpna
```

```
[SwitchD-vsi-vpna] gateway vsi-interface 1
[SwitchD-vsi-vpna] quit
```

Configuring DRNI

Configuring Switch A

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchA] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchA] drni system-mac 0001-0002-0003
[SwitchA] drni system-number 1
[SwitchA] drni system-priority 10
[SwitchA] drni restore-delay 180
[SwitchA] drni keepalive ip destination 60.1.1.2 source 60.1.1.1
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[SwitchA] interface bridge-aggregation 3
[SwitchA-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 to aggregation group 3.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchA-GigabitEthernet1/0/3] quit
```

Specify Bridge-Aggregation 3 as the IPP.

```
[SwitchA] interface bridge-aggregation 3
[SwitchA-Bridge-Aggregation3] port drni intra-portal-port 1
[SwitchA-Bridge-Aggregation3] undo mac-address static source-check enable
[SwitchA-Bridge-Aggregation3] quit
```

Disable the static source check feature on GigabitEthernet 1/0/5.

```
[SwitchA] interface gigabitethernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] undo mac-address static source-check enable
[SwitchA-GigabitEthernet1/0/5] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchA-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port drni group 4
[SwitchA-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] link-aggregation mode dynamic
```

```
[SwitchA-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchA-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port drni group 5
[SwitchA-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface loopback 0
[SwitchA] drni mad exclude interface loopback 1
[SwitchA] drni mad exclude interface gigabitethernet 1/0/4
[SwitchA] drni mad exclude interface gigabitethernet 1/0/5
[SwitchA] drni mad exclude interface vlan-interface 11
[SwitchA] drni mad exclude interface vsi-interface 1
[SwitchA] drni mad exclude interface vsi-interface 2
```

Configuring Switch B

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchB] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchB] drni system-mac 0001-0002-0003
[SwitchB] drni system-number 2
[SwitchB] drni system-priority 10
[SwitchB] drni restore-delay 180
[SwitchB] drni keepalive ip destination 60.1.1.1 source 60.1.1.2
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 3.

```
[SwitchB] interface bridge-aggregation 3
[SwitchB-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 to aggregation group 3.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchB-GigabitEthernet1/0/3] quit
```

Specify Bridge-Aggregation 3 as the IPP.

```
[SwitchB] interface bridge-aggregation 3
[SwitchB-Bridge-Aggregation3] port drni intra-portal-port 1
[SwitchB-Bridge-Aggregation3] undo mac-address static source-check enable
[SwitchB-Bridge-Aggregation3] quit
```

Disable the static source check feature on GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] undo mac-address static source-check enable
[SwitchB-GigabitEthernet1/0/5] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchB] interface bridge-aggregation 4
```

```
[SwitchB-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port drni group 4
[SwitchB-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchB-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port drni group 5
[SwitchB-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface loopback 0
[SwitchB] drni mad exclude interface loopback 1
[SwitchB] drni mad exclude interface gigabitethernet 1/0/4
[SwitchB] drni mad exclude interface gigabitethernet 1/0/5
[SwitchB] drni mad exclude interface vsi-interface 1
[SwitchB] drni mad exclude interface vsi-interface 2
[SwitchB] drni mad exclude interface vlan-interface 12
```

Configuring BGP to advertise BGP EVPN routes

Configuring Switch A

Configure BGP to advertise BGP EVPN routes.

```
[SwitchA] bgp 200
[SwitchA-bgp-default] peer 3.3.3.3 as-number 200
[SwitchA-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchA-bgp-default] address-family l2vpn evpn
[SwitchA-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchA-bgp-default-evpn] quit
[SwitchA-bgp-default] quit
```

Configuring Switch B

Configure BGP to advertise BGP EVPN routes.

```
[SwitchB] bgp 200
```

```
[SwitchB-bgp-default] peer 3.3.3.3 as-number 200
[SwitchB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] quit
```

Configuring Switch C

Configure BGP to advertise BGP EVPN routes and configure the switch as an RR.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] group evpn
[SwitchC-bgp-default] peer 1.1.1.1 group evpn
[SwitchC-bgp-default] peer 2.2.2.2 group evpn
[SwitchC-bgp-default] peer 4.4.4.4 group evpn
[SwitchC-bgp-default] peer evpn as-number 200
[SwitchC-bgp-default] peer evpn connect-interface loopback 0
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] peer evpn enable
[SwitchC-bgp-default-evpn] undo policy vpn-target
[SwitchC-bgp-default-evpn] peer evpn reflect-client
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] quit
```

Configuring Switch D

Configure BGP to advertise BGP EVPN routes.

```
[SwitchD] bgp 200
[SwitchD-bgp-default] peer 3.3.3.3 as-number 200
[SwitchD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchD-bgp-default] address-family l2vpn evpn
[SwitchD-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchD-bgp-default-evpn] quit
[SwitchD-bgp-default] quit
```

Mapping Ethernet service instances to VSIs

Configuring Switch A

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchA-Bridge-Aggregation4] service-instance 1000
[SwitchA-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchA-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port link-type trunk
```

```
[SwitchA-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchA-Bridge-Aggregation5] service-instance 1000
[SwitchA-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpnb**.

```
[SwitchA-Bridge-Aggregation5-srv1000] xconnect vsi vpnb
[SwitchA-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch B

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port link-type trunk
[SwitchB-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchB-Bridge-Aggregation4] service-instance 1000
[SwitchB-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port link-type trunk
[SwitchB-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchB-Bridge-Aggregation5] service-instance 1000
[SwitchB-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpnb**.

```
[SwitchB-Bridge-Aggregation5-srv1000] xconnect vsi vpnb
[SwitchB-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch D

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchD-GigabitEthernet1/0/1] service-instance 1000
[SwitchD-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchD-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchD-GigabitEthernet1/0/1-srv1000] quit
```

Verifying the configuration

Verifying the configuration on a DR member device

The verification procedure uses Switch A as an example.

Verify that Switch A has BGP EVPN routes.

```
[Switch A]display bgp l2vpn evpn
 BGP local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - dampened, h - history
```

```
              s - suppressed, S - stale, i - internal, e - external
              a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
 Total number of routes from all PEs: 2
 Route distinguisher: 1:1(vpna)
 Total number of routes: 2
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [5][0][24][10.1.1.0]/80
                        1.2.3.4         0          100        32768   i
* >  [5][0][24][10.1.2.0]/80
                        1.2.3.4         0          100        32768   i
 Route distinguisher: 1:10
 Total number of routes: 2
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][4.4.4.4]/80
                        4.4.4.4         0          100        0       i
 Route distinguisher: 1:20
 Total number of routes: 2
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][4.4.4.4]/80
                        4.4.4.4         0          100        0       i
```

Verify that the VXLAN tunnel to Switch D is up, and the source address of the tunnel is the virtual VTEP address.

```
[SwitchA] display interface Tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.2.3.4, destination 4.4.4.4
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Verify that ACs have been created on the IPP and mapped to VXLAN 10 and VXLAN 20.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: Auto_L3VNI1000_3
  VSI Index               : 1
```

```
  VSI State               : Down
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 3
  VXLAN ID                : 1000

VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 1
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel0              0x5000000  UP       Auto        Disabled
  ACs:
    AC                              Link ID  State       Type
    BAGG4 srv1000                   0        Up          Manual
    BAGG3 srv2                      1        Up          Dynamic (DRNI)

VSI Name: vpnb
  VSI Index               : 2
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
```

```
MAC Table Limit         : -
MAC Learning rate       : -
Drop Unknown            : -
Flooding                : Enabled
Statistics              : Disabled
Gateway Interface       : VSI-interface 2
VXLAN ID                : 20
Tunnels:
  Tunnel Name          Link ID    State    Type        Flood proxy
  Tunnel0              0x5000000  UP       Auto        Disabled
ACs:
  AC                              Link ID  State       Type
  BAGG5 srv1000                   0        Up          Manual
  BAGG3 srv3                      1        Up          Dynamic (DRNI)
```

Verifying the network connectivity of the VMs

Verify that the VMs can communicate when both Switch A and Switch B are operating correctly. (Details not shown.)

Verify that VM 1 and VM 5 can communicate when Switch A's or Switch B's links to the local site are disconnected. (Details not shown.)

Configuration files

- Switch A:

```
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
```

```
#
vlan 11
#
vlan 100
#
 l2vpn enable
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
 evpn global-mac 0002-0003-0004
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
```

```
  encapsulation s-vid 3
  xconnect vsi vpnb
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 60.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-aggregation group 3
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 11
 undo stp enable
 undo mac-address static source-check enable
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
```

```
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 ip address 10.1.2.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni keepalive ip destination 60.1.1.2 source 60.1.1.1
 drni restore-delay 180
 drni system-mac 0001-0002-0003
 drni system-number 1
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/4
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface 11
 drni mad exclude interface Vsi-interface1
 drni mad exclude interface Vsi-interface2
#
return
```

- Switch B:

```
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
```

```
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 12
#
vlan 100
#
 l2vpn enable
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
 evpn global-mac 0002-0003-0004
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation3
 link-aggregation mode dynamic
 port drni intra-portal-port 1
 undo mac-address static source-check enable
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
```

```
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpnb
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 60.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-aggregation group 3
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 12
```

```
 undo stp enable
 undo mac-address static source-check enable
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 ip address 10.1.2.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni keepalive ip destination 60.1.1.1 source 60.1.1.2
 drni restore-delay 180
 drni system-mac 0001-0002-0003
 drni system-number 2
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/4
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Vlan-interface 12
 drni mad exclude interface Vsi-interface1
 drni mad exclude interface Vsi-interface2
#
return
```

- Switch C:

```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 11.1.1.0 0.0.0.255
```

```
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 11 to 13
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.3 255.255.255.0
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
bgp 200
 group evpn internal
 peer evpn connect-interface LoopBack0
 peer 1.1.1.1 group evpn
 peer 2.2.2.2 group evpn
 peer 4.4.4.4 group evpn
 #
 address-family l2vpn evpn
  undo policy vpn-target
  peer evpn enable
  peer evpn reflect-client
#
return
```

- Switch D:

```
#
```

```
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
vlan 2
#
vlan 13
#
l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
return
```

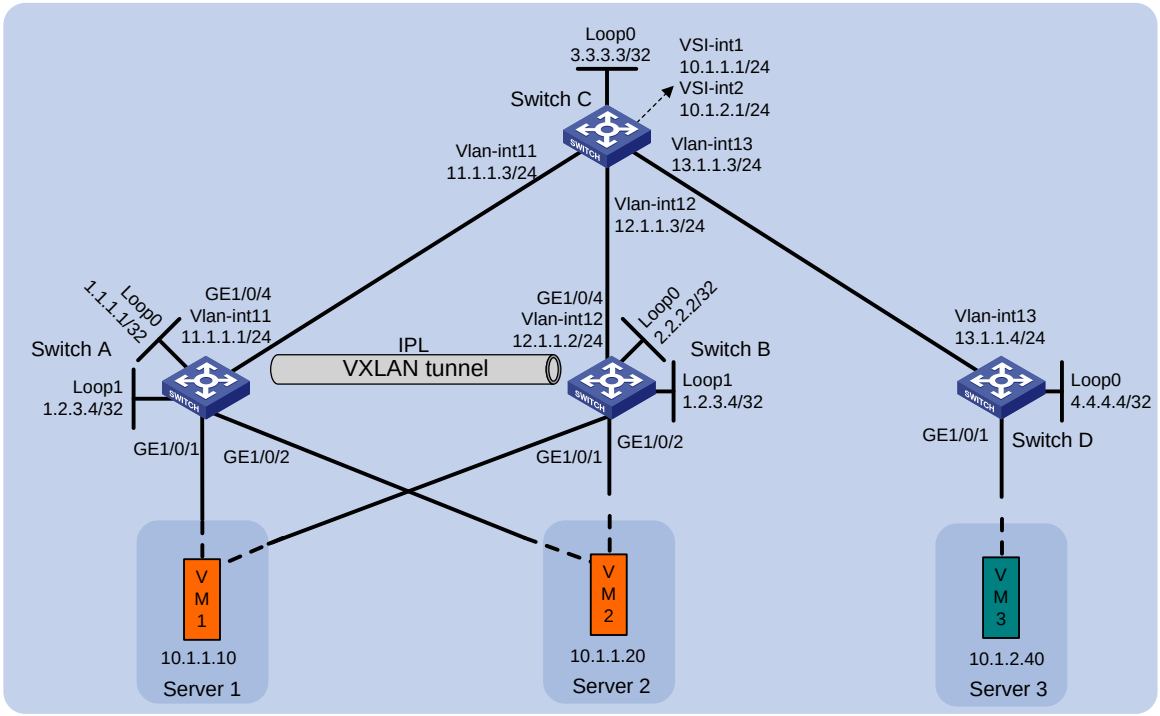
Example: Configuring DRNI using a VXLAN tunnel as the IPL on EVPN gateways

Network configuration

As shown in Figure 4, perform the following tasks to make sure the VMs can communicate with one another:

- Configure VXLAN 10 on Switch A, Switch B, and Switch D, and configure VXLAN 20 on Switch A, and Switch B.
- Configure Switch A, Switch B, and Switch D as distributed EVPN gateways to provide Layer 3 forwarding service for VMs.
- Configure DRNI on Switch A and Switch B to virtualize them into one VTEP. Manually set up a VXLAN tunnel as the IPL between the switches.
- Create a monitor link group on Switch A and Switch B. Configure the transport-facing interfaces of Switch A and Switch B as uplink interfaces for the monitor link group, and member interfaces of DR interfaces as downlink interfaces.
- Configure Switch C as an RR.

Figure 4 Network diagram



Analysis

To make sure the overlay network has connectivity,, configure a routing protocol on these switches to advertise routes for reaching their interfaces, including the loopback interfaces. In this example, OSPF is used.

To conserve resources, configure Switch C to reflect routes for Switch A, Switch B, and Switch D.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series	Not supported

Hardware	Software version
S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

Make sure the following settings are consistent on the DR member devices:

- Ethernet service instances and their match criterion on the DR interfaces in the same DR group or single-homed site-facing interfaces.
- VXLAN IDs of VSIs.

In addition, the Ethernet service instances must be created manually.

As a best practice, do not redistribute external routes on the DR member devices.

Use the **drni mad exclude interface** command to exclude all interfaces used by EVPN from the shutdown action by DRNI MAD. The interfaces include VSI interfaces, interfaces that provide BGP peer addresses, interfaces used for setting up the keepalive link, and transport-facing outgoing interfaces of VXLAN tunnels.

Use the **drni mad exclude interface** command to exclude VXLAN tunnel interfaces and their traffic outgoing interfaces from the MAD shutdown action by DRNI before you configure them as IPPs. If you have configured the VXLAN tunnel interfaces as IPPs before excluding them and their traffic outgoing interfaces from the MAD shutdown action, you must first remove the IPP configuration. After the VXLAN tunnel interfaces and their traffic outgoing interfaces come up, exclude the interfaces from the MAD shutdown action by DRNI. Then, configure the VXLAN tunnel interfaces as IPPs.

For EVPN to run correctly on a DR system, you must execute the **undo mac-address static source-check enable** command to disable static source check on the following interfaces:

- Layer 2 aggregate interfaces or Layer 2 Ethernet interfaces acting as the IPPs.
- Transport-facing physical interfaces.

As a best practice, use the IP address of a loopback interface as the virtual VTEP address.

You must disable spanning tree on the Layer 2 Ethernet interface that acts as the physical traffic outgoing interface of a VXLAN tunnel. If you enable spanning tree on that interface, the upstream device will falsely block the interfaces connected to the DR member devices.

Procedures

Configuring the system operating mode

Set the system operating mode to VXLAN on Switch A, and reboot the switch for the mode change to take effect.

```
<SwitchA> system-view
[SwitchA] switch-mode 1
Reboot device to make the configuration take effect.
[SwitchA] quit
<SwitchA> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Set the system operating mode of Switch B and Switch D to VXLAN. The method is the same as Switch A. (Details not shown.)

Configuring Layer 3 interfaces

Configure the Layer 3 interfaces on Switch A.

```
[SwitchA] interface loopback 0
[SwitchA-Loopback0] ip address 1.1.1.1 32
[SwitchA-Loopback0] quit
[SwitchA] interface loopback 1
[SwitchA-Loopback1] ip address 1.2.3.4 32
[SwitchA-Loopback1] quit
[SwitchA] vlan 11
[SwitchA-vlan11] port gigabitethernet 1/0/5
[SwitchA-vlan11] quit
[SwitchA] interface vlan-interface 11
[SwitchA-Vlan-interface11] ip address 11.1.1.1 24
[SwitchA-Vlan-interface11] quit
```

Configure the Layer 3 interfaces on other switches. (Details not shown.)

On VM 1, VM 3, and VM 5, specify 10.1.1.1 as the gateway address. On VM 2 and VM 4, specify 10.1.2.1 as the gateway address. (Details not shown.)

Configuring OSPF

Configuring Switch A

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configuring Switch B

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 1.2.3.4 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configuring Switch C

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configuring Switch D

Configure OSPF to advertise the networks attached to the Layer 3 interfaces.

```
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 13.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Disabling spanning tree

Configuring Switch A

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/4.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] undo stp enable
[SwitchA-GigabitEthernet1/0/4] quit
```

Configuring Switch B

Disable spanning tree on transport-facing physical interface GigabitEthernet 1/0/4.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] undo stp enable
```

```
[SwitchB-GigabitEthernet1/0/4] quit
```

Configuring EVPN

Configuring Switch A

Enable L2VPN.

```
[SwitchA] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchA] vxlan tunnel mac-learning disable
[SwitchA] vxlan tunnel arp-learning disable
```

Specify the reserved VXLAN as VXLAN 1234.

```
[SwitchA] reserved vxlan 1234
```

Configure the EVPN global MAC address as **0002-0003-0004**.

```
[SwitchA] evpn global-mac 2-3-4
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
```

Create an EVPN instance on VSI **vpnb**.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchA-vsi-vpnb-evpn-vxlan] route-distinguisher auto
[SwitchA-vsi-vpnb-evpn-vxlan] vpn-target auto
[SwitchA-vsi-vpnb-evpn-vxlan] quit
```

Create VXLAN 20.

```
[SwitchA-vsi-vpnb] vxlan 20
[SwitchA-vsi-vpnb-vxlan-20] quit
[SwitchA-vsi-vpnb] quit
```

Configuring Switch B

Enable L2VPN.

```
[SwitchB] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchB] vxlan tunnel mac-learning disable
[SwitchB] vxlan tunnel arp-learning disable
```

Specify the reserved VXLAN as VXLAN 1234.

```
[SwitchB] reserved vxlan 1234
```

Configure the EVPN global MAC address as **0002-0003-0004**.

```
[SwitchB] evpn global-mac 2-3-4
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
```

Create an EVPN instance on VSI **vpnb**.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchB-vsi-vpnb-evpn-vxlan] route-distinguisher auto
[SwitchB-vsi-vpnb-evpn-vxlan] vpn-target auto
[SwitchB-vsi-vpnb-evpn-vxlan] quit
```

Create VXLAN 20.

```
[SwitchB-vsi-vpnb] vxlan 20
[SwitchB-vsi-vpnb-vxlan-20] quit
[SwitchB-vsi-vpnb] quit
```

Configuring Switch D

Enable L2VPN.

```
[SwitchD] l2vpn enable
```

Disable remote MAC address learning and remote ARP learning.

```
[SwitchD] vxlan tunnel mac-learning disable
[SwitchD] vxlan tunnel arp-learning disable
```

Create an EVPN instance on VSI **vpna**.

```
[SwitchD] vsi vpna
[SwitchD-vsi-vpna] evpn encapsulation vxlan
```

Configure the switch to automatically generate an RD and a route target for the EVPN instance.

```
[SwitchD-vsi-vpna-evpn-vxlan] route-distinguisher auto
[SwitchD-vsi-vpna-evpn-vxlan] vpn-target auto
[SwitchD-vsi-vpna-evpn-vxlan] quit
```

Create VXLAN 10.

```
[SwitchD-vsi-vpna] vxlan 10
[SwitchD-vsi-vpna-vxlan-10] quit
[SwitchD-vsi-vpna] quit
```

Configuring distributed EVPN gateways

Configuring Switch A

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchA] ip vpn-instance vpna
[SwitchA-vpn-instance-vpna] route-distinguisher 1:1
[SwitchA-vpn-instance-vpna] address-family ipv4
[SwitchA-vpn-ipv4-vpna] vpn-target 2:2
[SwitchA-vpn-ipv4-vpna] quit
[SwitchA-vpn-instance-vpna] address-family evpn
[SwitchA-vpn-evpn-vpna] vpn-target 1:1
[SwitchA-vpn-evpn-vpna] quit
[SwitchA-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchA] interface vsi-interface 1
[SwitchA-Vsi-interface1] ip binding vpn-instance vpna
[SwitchA-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[SwitchA-Vsi-interface1] mac-address 1-1-1
[SwitchA-Vsi-interface1] distributed-gateway local
[SwitchA-Vsi-interface1] local-proxy-arp enable
[SwitchA-Vsi-interface1] quit
```

Configure VSI-interface 2 as a distributed gateway.

```
[SwitchA] interface vsi-interface 2
[SwitchA-Vsi-interface2] ip binding vpn-instance vpna
[SwitchA-Vsi-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchA-Vsi-interface2] mac-address 2-2-2
[SwitchA-Vsi-interface2] distributed-gateway local
[SwitchA-Vsi-interface2] local-proxy-arp enable
[SwitchA-Vsi-interface2] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchA] interface vsi-interface 3
[SwitchA-Vsi-interface3] ip binding vpn-instance vpna
[SwitchA-Vsi-interface3] l3-vni 1000
[SwitchA-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] gateway vsi-interface 1
[SwitchA-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for VSI **vpnb**.

```
[SwitchA] vsi vpnb
[SwitchA-vsi-vpnb] gateway vsi-interface 2
[SwitchA-vsi-vpnb] quit
```

Configuring Switch B

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchB] ip vpn-instance vpna
[SwitchB-vpn-instance-vpna] route-distinguisher 1:1
[SwitchB-vpn-instance-vpna] address-family ipv4
[SwitchB-vpn-ipv4-vpna] vpn-target 2:2
[SwitchB-vpn-ipv4-vpna] quit
[SwitchB-vpn-instance-vpna] address-family evpn
```

```
[SwitchB-vpn-evpn-vpna] vpn-target 1:1
[SwitchB-vpn-evpn-vpna] quit
[SwitchB-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchB] interface vsi-interface 1
[SwitchB-Vsi-interface1] ip binding vpn-instance vpna
[SwitchB-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[SwitchB-Vsi-interface1] mac-address 1-1-1
[SwitchB-Vsi-interface1] distributed-gateway local
[SwitchB-Vsi-interface1] local-proxy-arp enable
[SwitchB-Vsi-interface1] quit
```

Configure VSI-interface 2 as a distributed gateway.

```
[SwitchB] interface vsi-interface 2
[SwitchB-Vsi-interface2] ip binding vpn-instance vpna
[SwitchB-Vsi-interface2] ip address 10.1.2.1 255.255.255.0
[SwitchB-Vsi-interface2] mac-address 2-2-2
[SwitchB-Vsi-interface2] distributed-gateway local
[SwitchB-Vsi-interface2] local-proxy-arp enable
[SwitchB-Vsi-interface2] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchB] interface vsi-interface 3
[SwitchB-Vsi-interface3] ip binding vpn-instance vpna
[SwitchB-Vsi-interface3] l3-vni 1000
[SwitchB-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] gateway vsi-interface 1
[SwitchB-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for VSI **vpnb**.

```
[SwitchB] vsi vpnb
[SwitchB-vsi-vpnb] gateway vsi-interface 2
[SwitchB-vsi-vpnb] quit
```

Configuring Switch D

Configure RD and route target settings for VPN instance **vpna**.

```
[SwitchD] ip vpn-instance vpna
[SwitchD-vpn-instance-vpna] route-distinguisher 1:1
[SwitchD-vpn-instance-vpna] address-family ipv4
[SwitchD-vpn-ipv4-vpna] vpn-target 2:2
[SwitchD-vpn-ipv4-vpna] quit
[SwitchD-vpn-instance-vpna] address-family evpn
[SwitchD-vpn-evpn-vpna] vpn-target 1:1
[SwitchD-vpn-evpn-vpna] quit
[SwitchD-vpn-instance-vpna] quit
```

Configure VSI-interface 1 as a distributed gateway.

```
[SwitchD] interface vsi-interface 1
[SwitchD-Vsi-interface1] ip binding vpn-instance vpna
```

```
[SwitchD-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[SwitchD-Vsi-interface1] mac-address 1-1-1
[SwitchD-Vsi-interface1] distributed-gateway local
[SwitchD-Vsi-interface1] local-proxy-arp enable
[SwitchD-Vsi-interface1] quit
```

Create VSI-interface 3. Associate VSI-interface 3 with VPN instance **vpna**, and configure the L3 VXLAN ID as 1000 for the VPN instance.

```
[SwitchD] interface vsi-interface 3
[SwitchD-Vsi-interface3] ip binding vpn-instance vpna
[SwitchD-Vsi-interface3] l3-vni 1000
[SwitchD-Vsi-interface3] quit
```

Specify VSI-interface 1 as the gateway interface for VSI **vpna**.

```
[SwitchD] vsi vpna
[SwitchD-vsi-vpna] gateway vsi-interface 1
[SwitchD-vsi-vpna] quit
```

Configuring DRNI

Configuring Switch A

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchA] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchA] drni system-mac 0001-0002-0003
[SwitchA] drni system-number 1
[SwitchA] drni system-priority 10
[SwitchA] drni restore-delay 180
```

Create a tunnel to Switch B, and set the ToS of tunneled packets to 100.

```
[SwitchA] interface tunnel 1 mode vxlan
[SwitchA-Tunnel1] source 1.1.1.1
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] tunnel tos 100
[SwitchA-Tunnel1] quit
```

Exclude Tunnel 1 from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface tunnel 1
```

Specify Tunnel 1 as the IPP

```
[SwitchA] interface tunnel 1
[SwitchA-Tunnel1] port drni intra-portal-port 1
[SwitchA-Tunnel1] quit
```

Disable the static source check feature on GigabitEthernet 1/0/4.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] undo mac-address static source-check enable
[SwitchA-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchA-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port drni group 4
[SwitchA-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchA-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port drni group 5
[SwitchA-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchA] drni mad exclude interface loopback0
[SwitchA] drni mad exclude interface gigabitethernet1/0/4
[SwitchA] drni mad exclude interface vsi-interface 1
[SwitchA] drni mad exclude interface vsi-interface 2
[SwitchA] drni mad exclude interface vlan-interface 11
```

Configuring Switch B

Specify the virtual VTEP address as 1.2.3.4.

```
[SwitchB] evpn drni group 1.2.3.4
```

Configure DR system parameters.

```
[SwitchB] drni system-mac 0001-0002-0003
[SwitchB] drni system-number 2
[SwitchB] drni system-priority 10
[SwitchB] drni restore-delay 180
```

Create a tunnel to Switch A, and set the ToS of tunneled packets to 100.

```
[SwitchB] interface tunnel 1 mode vxlan
[SwitchB-Tunnel1] source 2.2.2.2
[SwitchB-Tunnel1] destination 1.1.1.1
[SwitchB-Tunnel1] tunnel tos 100
[SwitchB-Tunnel1] quit
```

Exclude Tunnel 1 from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface tunnel 1
```

Specify Tunnel 1 as the IPP

```
[SwitchB] interface tunnel 1
[SwitchB-Tunnel1] port drni intra-portal-port 1
```

```
[SwitchB-Tunnel1] quit
```

Disable the static source check feature on GigabitEthernet 1/0/4.

```
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] undo mac-address static source-check enable
[SwitchB-GigabitEthernet1/0/4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 4.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 4
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign Bridge-Aggregation 4 to DR group 4.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port drni group 4
[SwitchB-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 5.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 5
[SwitchB-GigabitEthernet1/0/2] quit
```

Assign Bridge-Aggregation 5 to DR group 5.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port drni group 5
[SwitchB-Bridge-Aggregation5] quit
```

Exclude all interfaces used by EVPN from the shutdown action by DRNI MAD.

```
[SwitchB] drni mad exclude interface loopback0
[SwitchB] drni mad exclude interface gigabitethernet1/0/4
[SwitchB] drni mad exclude interface vsi-interface 1
[SwitchB] drni mad exclude interface vsi-interface 2
[SwitchB] drni mad exclude interface vlan-interface 12
```

Configuring BGP to advertise BGP EVPN routes

Configuring Switch A

Configure BGP to advertise BGP EVPN routes.

```
[SwitchA] bgp 200
[SwitchA-bgp-default] peer 3.3.3.3 as-number 200
[SwitchA-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchA-bgp-default] address-family l2vpn evpn
[SwitchA-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchA-bgp-default-evpn] quit
```

```
[SwitchA-bgp-default] quit
```

Configuring Switch B

Configure BGP to advertise BGP EVPN routes.

```
[SwitchB] bgp 200
[SwitchB-bgp-default] peer 3.3.3.3 as-number 200
[SwitchB-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchB-bgp-default] address-family l2vpn evpn
[SwitchB-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchB-bgp-default-evpn] quit
[SwitchB-bgp-default] quit
```

Configuring Switch C

Configure BGP to advertise BGP EVPN routes and configure the switch as an RR.

```
[SwitchC] bgp 200
[SwitchC-bgp-default] group evpn
[SwitchC-bgp-default] peer 1.1.1.1 group evpn
[SwitchC-bgp-default] peer 2.2.2.2 group evpn
[SwitchC-bgp-default] peer 4.4.4.4 group evpn
[SwitchC-bgp-default] peer evpn as-number 200
[SwitchC-bgp-default] peer evpn connect-interface loopback 0
[SwitchC-bgp-default] address-family l2vpn evpn
[SwitchC-bgp-default-evpn] peer evpn enable
[SwitchC-bgp-default-evpn] undo policy vpn-target
[SwitchC-bgp-default-evpn] peer evpn reflect-client
[SwitchC-bgp-default-evpn] quit
[SwitchC-bgp-default] quit
```

Configuring Switch D

Configure BGP to advertise BGP EVPN routes.

```
[SwitchD] bgp 200
[SwitchD-bgp-default] peer 3.3.3.3 as-number 200
[SwitchD-bgp-default] peer 3.3.3.3 connect-interface loopback 0
[SwitchD-bgp-default] address-family l2vpn evpn
[SwitchD-bgp-default-evpn] peer 3.3.3.3 enable
[SwitchD-bgp-default-evpn] quit
[SwitchD-bgp-default] quit
```

Mapping Ethernet service instances to VSIs

Configuring Switch A

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchA] interface bridge-aggregation 4
[SwitchA-Bridge-Aggregation4] port link-type trunk
[SwitchA-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchA-Bridge-Aggregation4] service-instance 1000
[SwitchA-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchA-Bridge-Aggregation4-srv1000] xconnect vsi vpna
```

```
[SwitchA-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchA] interface bridge-aggregation 5
[SwitchA-Bridge-Aggregation5] port link-type trunk
[SwitchA-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchA-Bridge-Aggregation5] service-instance 1000
[SwitchA-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpnb**.

```
[SwitchA-Bridge-Aggregation5-srv1000] xconnect vsi vpnb
[SwitchA-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch B

On Bridge-Aggregation 4, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface bridge-aggregation 4
[SwitchB-Bridge-Aggregation4] port link-type trunk
[SwitchB-Bridge-Aggregation4] port trunk permit vlan 2
[SwitchB-Bridge-Aggregation4] service-instance 1000
[SwitchB-Bridge-Aggregation4-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchB-Bridge-Aggregation4-srv1000] xconnect vsi vpna
[SwitchB-Bridge-Aggregation4-srv1000] quit
```

On Bridge-Aggregation 5, create Ethernet service instance 1000 to match VLAN 3.

```
[SwitchB] interface bridge-aggregation 5
[SwitchB-Bridge-Aggregation5] port link-type trunk
[SwitchB-Bridge-Aggregation5] port trunk permit vlan 3
[SwitchB-Bridge-Aggregation5] service-instance 1000
[SwitchB-Bridge-Aggregation5-srv1000] encapsulation s-vid 3
```

Map Ethernet service instance 1000 to VSI **vpnb**.

```
[SwitchB-Bridge-Aggregation5-srv1000] xconnect vsi vpnb
[SwitchB-Bridge-Aggregation5-srv1000] quit
```

Configuring Switch D

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchD] interface gigabitethernet 1/0/1
[SwitchD-GigabitEthernet1/0/1] port link-type trunk
[SwitchD-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchD-GigabitEthernet1/0/1] service-instance 1000
[SwitchD-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchD-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchD-GigabitEthernet1/0/1-srv1000] quit
```

Configuring Monitor Link

Configuring Switch A

Create monitor link group 1 and assign the uplink and downlink interfaces to it.

```
[SwitchA] monitor-link group 1
```

```
[SwitchA-mtlk-group1] port gigabitethernet 1/0/1 downlink
[SwitchA-mtlk-group1] port gigabitethernet 1/0/2 downlink
[SwitchA-mtlk-group1] port gigabitethernet 1/0/4 uplink
[SwitchA-mtlk-group1] quit
```

Configuring Switch B

Create monitor link group 1 and assign the uplink and downlink interfaces to it.

```
[SwitchB] monitor-link group 1
[SwitchB-mtlk-group1] port gigabitethernet 1/0/1 downlink
[SwitchB-mtlk-group1] port gigabitethernet 1/0/2 downlink
[SwitchB-mtlk-group1] port gigabitethernet 1/0/4 uplink
[SwitchB-mtlk-group1] quit
```

Verifying the configuration

Verifying the configuration on a DR member device

The verification procedure uses Switch A as an example.

Verify that Switch A has BGP EVPN routes.

```
[Switch A]display bgp l2vpn evpn
 BGP local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - dampened, h - history
               s - suppressed, S - stale, i - internal, e - external
               a - additional-path
       Origin: i - IGP, e - EGP, ? - incomplete
 Total number of routes from all PEs: 3
 Route distinguisher: 1:1(vpna)
 Total number of routes: 2
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [5][0][24][10.1.1.0]/80
                        1.1.1.1         0          100        32768   i
* >  [5][0][24][10.1.2.0]/80
                        1.1.1.1         0          100        32768   i
 Route distinguisher: 1:10
 Total number of routes: 4
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.1.1.1]/80
                        1.1.1.1         0          100        32768   i
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][2.2.2.2]/80
                        2.2.2.2         0          100        0       i
* >i [3][0][32][4.4.4.4]/80
                        4.4.4.4         0          100        0       i
 Route distinguisher: 1:20
```

```
 Total number of routes: 3
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn
* >  [3][0][32][1.1.1.1]/80
                        1.1.1.1         0          100        32768   i
* >  [3][0][32][1.2.3.4]/80
                        1.2.3.4         0          100        32768   i
* >i [3][0][32][2.2.2.2]/80
                        2.2.2.2         0          100        0       i
```

Verify that the IPL Tunnel 1 is up, and Tunnel 0 to Switch D uses the virtual VTEP address as the source address.

```
[SwitchA] display interface tunnel
Tunnel0
Current state: UP
Line protocol state: UP
Description: Tunnel0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.2.3.4, destination 4.4.4.4
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 149 bytes/sec, 1192 bits/sec, 1 packets/sec
Last 300 seconds output rate: 379 bytes/sec, 3032 bits/sec, 3 packets/sec
Input: 398 packets, 46446 bytes, 0 drops
Output: 3597 packets, 363591 bytes, 0 drops
```

Verify that the VXLAN tunnels have been assigned to VXLAN 10 and VXLAN 20.

```
[SwitchA] display l2vpn vsi verbose
VSI Name: Auto_L3VNI1000_3
  VSI Index              : 1
  VSI State              : Down
  MTU                    : 1500
  Bandwidth              : -
  Broadcast Restrain     : -
```

```
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 3
  VXLAN ID                : 1000

VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 1
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel0              0x5000000  UP       Auto        Disabled
    Tunnel1              0x5000001  UP       Manual      Disabled
  ACs:
    AC                              Link ID  State       Type
    BAGG4 srv1000                   0        Up          Manual

VSI Name: vpnb
  VSI Index               : 2
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
```

```
Statistics              : Disabled
Gateway Interface       : VSI-interface 2
VXLAN ID                : 20
Tunnels:
  Tunnel Name          Link ID    State    Type        Flood proxy
  Tunnel1              0x5000001  UP       Manual      Disabled
ACs:
  AC                              Link ID  State       Type
  BAGG5 srv1000                   0        Up          Manual
```

Verifying the network connectivity of the VMs

Verify that the VMs can communicate when both Switch A and Switch B are operating correctly. (Details not shown.)

Verify that VM 1 and VM 5 can communicate when Switch A's or Switch B's links to the local site are disconnected. (Details not shown.)

Configuration files

- Switch A:

```
#
monitor-link group 1
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 11
#
```

```
 l2vpn enable
 reserved vxlan 1234
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
 evpn global-mac 0002-0003-0004
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpnb
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
#
```

```
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-aggregation group 4
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port link-aggregation group 5
 port monitor-link group 1 downlink
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 11
 undo stp enable
 port monitor-link group 1 uplink
 undo mac-address static source-check enable
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 ip address 10.1.2.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
interface Tunnel1 mode vxlan
 port drni intra-portal-port 1
 source 1.1.1.1
 destination 2.2.2.2
 tunnel tos 100
#
```

```
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni restore-delay 180
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Tunnel1
 drni mad exclude interface Vlan-interface 11
 drni mad exclude interface Vsi-interface1
 drni mad exclude interface Vsi-interface2
#
return
```

- Switch B:

```
#
monitor-link group 1
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 1.2.3.4 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.1.1.0 0.0.0.255
#
vlan 2
#
vlan 3
#
vlan 12
```

```
#
 l2vpn enable
 reserved vxlan 1234
 vxlan tunnel arp-learning disable
 evpn drni group 1.2.3.4
 evpn global-mac 0002-0003-0004
#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port drni group 4
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface Bridge-Aggregation5
 port link-type trunk
 port trunk permit vlan 1 3
 link-aggregation mode dynamic
 port drni group 5
 #
 service-instance 1000
  encapsulation s-vid 3
  xconnect vsi vpnb
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack1
 ip address 1.2.3.4 255.255.255.255
```

```
#
interface Vlan-interface12
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 port monitor-link group 1 downlink
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 port monitor-link group 1 downlink
 port link-aggregation group 5
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 12
 undo stp enable
 port monitor-link group 1 uplink
 undo mac-address static source-check enable
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpna
 ip address 10.1.2.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
interface Tunnel1 mode vxlan
 port drni intra-portal-port 1
 source 2.2.2.2
 destination 1.1.1.1
 tunnel tos 100
```

```
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
 drni restore-delay 180
 drni system-mac 0001-0002-0003
 drni system-number 2
 drni system-priority 10
#
 drni mad exclude interface LoopBack0
 drni mad exclude interface GigabitEthernet1/0/5
 drni mad exclude interface Tunnel1
 drni mad exclude interface Vlan-interface 12
 drni mad exclude interface Vsi-interface1
 drni mad exclude interface Vsi-interface2
#
return
```

- Switch C:

```
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 11.1.1.0 0.0.0.255
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
#
vlan 11 to 13
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 12.1.1.3 255.255.255.0
#
interface Vlan-interface13
 ip address 13.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
#
```

```
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 12
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 13
#
bgp 200
 group evpn internal
 peer evpn connect-interface LoopBack0
 peer 1.1.1.1 group evpn
 peer 2.2.2.2 group evpn
 peer 4.4.4.4 group evpn
 #
 address-family l2vpn evpn
  undo policy vpn-target
  peer evpn enable
  peer evpn reflect-client
#
return
```

- Switch D:

```
#
ip vpn-instance vpna
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 13.1.1.0 0.0.0.255
#
vlan 2
#
vlan 13
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
```

```
vsi vpna
 gateway vsi-interface 1
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface13
 ip address 13.1.1.4 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
 port link-mode bridge
 #
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 13
#
interface Vsi-interface1
 ip binding vpn-instance vpna
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local
#
interface Vsi-interface3
 ip binding vpn-instance vpna
 l3-vni 1000
#
bgp 200
 peer 3.3.3.3 as-number 200
 peer 3.3.3.3 connect-interface LoopBack0
 #
 address-family l2vpn evpn
  peer 3.3.3.3 enable
#
return
```

Contents

Introduction

This document provides multicast VPN configuration examples.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of multicast VPN.

Example: Configuring intra-AS MDT-based MVPN

Network configuration

As shown in Figure 1:

- Customer A has two branches that connect to the MPLS L3VPN network of a service provider.
- PIM-SM runs within the two branches.
- The multicast source and the receiver host are in different branches.

Configure intra-AS MDT-based MVPN so that the receiver host can receive the multicast data from the source.

Figure 1 Network diagram

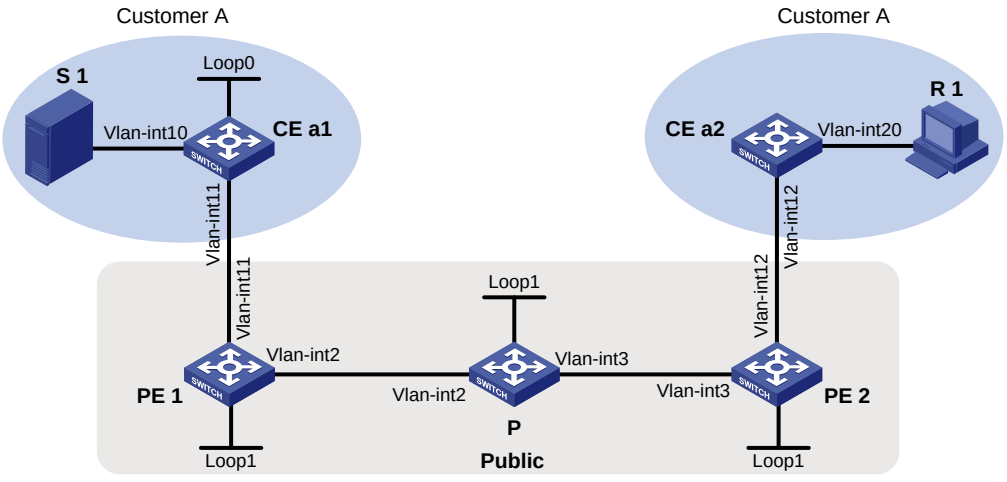


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.11.3.2/24	PE 2	Vlan-int3	192.168.2.2/24
PE 1	Vlan-int2	192.168.1.2/24	PE 2	Vlan-int12	10.11.2.1/24
PE 1	Vlan-int11	10.11.1.1/24	PE 2	Loop1	1.1.1.2/32

Device	Interface	IP address	Device	Interface	IP address
PE 1	Loop1	1.1.1.1/32	CE a1	Vlan-int10	10.11.3.1/24
P	Vlan-int2	192.168.1.1/24	CE a1	Vlan-int11	10.11.1.2/24
P	Vlan-int3	192.168.2.1/24	CE a1	Loop0	2.2.2.2/32
P	Loop1	3.3.3.3/32	CE a2	Vlan-int20	10.11.4.1/24
R 1	—	10.11.4.2/24	CE a2	Vlan-int12	10.11.2.2/24

Analysis

To meet the network requirement, you must run PIM on the devices of the public network, and configure MDT-based MVPN on each PE. In addition, make sure the PIM protocol on the public network is independent from the PIM protocol for the VPN instance.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series	Not supported

Hardware	Software version
S5560S-SI switch series	
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported

Hardware	Software version
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure the intra-AS MDT-based MVPN, follow these restrictions and guidelines:

- The MTI interfaces take effect only after the default-group and the MVPN source interface are specified and the MVPN source interface obtains the public IP address.
- To ensure correct MTI forwarding, you must create a service loopback group and specify the multicast tunnel service type by using the **service-loopback group** command. For more information about this command, see *Layer 2—LAN Switching Command Reference.*
- You must enable the same PIM mode on all interfaces that belong to the same VPN instance (including the interfaces associated with the VPN instance on the PEs).
- You must specify the same default-group for the same VPN instance on different PEs.
- The IP address of the MVPN source interface must be the same as the source address used for establishing BGP peer relationship. Otherwise, correct routing information cannot be obtained.

Procedures

1. Assign an IP address and subnet mask to each interface on CE a1, as shown in Table 1.

```
<CEa1> system-view
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.11.3.1 24
[CEa1-Vlan-interface10] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.11.1.2 24
[CEa1-Vlan-interface11] quit
```

   # Configure PE 1, P, PE 2, and CE a2 in the same way CE a1 is configured. (Details not shown.)

2. Configure a unicast routing protocol and basic MPLS VPN on all devices so that all devices are interoperable at the network layer. (Details not shown.)

   For more information about configuring basic MPLS VPN, see *MPLS Configuration Guide*.

3. Enable IP multicast routing on the public network, and enable PIM-SM on the public network interfaces (including Loopback interfaces):

   # On PE 1, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE1] multicast routing
[PE1-mrib] quit
```

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

On P, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[P] multicast routing
[P-mrib] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] pim sm
[P-Vlan-interface2] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] pim sm
[P-Vlan-interface3] quit
[P] interface loopback 1
[P-LoopBack1] pim sm
[P-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[P] pim
[P-pim] c-bsr 3.3.3.3
[P-pim] c-rp 3.3.3.3
[P-pim] quit
```

On PE 2, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] pim sm
[PE2-Vlan-interface3] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

4. Enable IP multicast routing for the VPN instance, enable PIM-SM on the private network interfaces, and enable IGMP on interfaces that have receiver hosts attached:

On CE a1, enable IP multicast routing, and enable PIM-SM on each interface.

```
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
```

Configure Loopback 0 as a C-BSR and a C-RP.

```
[CEa1] pim
```

```
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

On CE a2, enable IP multicast routing, enable PIM-SM on VLAN-interface 12, and enable IGMP on the receiver-side interface VLAN-interface 20.

```
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface vlan-interface 12
[CEa2-Vlan-interface12] pim sm
[CEa2-Vlan-interface12] quit
[CEa2] interface vlan-interface 20
[CEa2-Vlan-interface20] igmp enable
[CEa2-Vlan-interface20] quit
```

On PE 1, create a VPN instance named **customerA**.

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 111:1
[PE1-vpn-instance-customerA] quit
```

Associate VLAN-interface 11 with VPN instance **customerA**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance customerA
[PE1-Vlan-interface11] quit
```

Enable IP multicast routing for VPN instance **customerA**.

```
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
```

Enable PIM-SM on VLAN-interface 11.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

On PE 2, create a VPN instance named **customerA**.

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 100:1
[PE2-vpn-instance-customerA] vpn-target 111:1
[PE2-vpn-instance-customerA] quit
```

Associate VLAN-interface 12 with VPN instance **customerA**.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] ip binding vpn-instance customerA
[PE2-Vlan-interface12] quit
```

Enable IP multicast routing for VPN instance **customerA**.

```
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
```

Enable PIM-SM on VLAN-interface 12.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] pim sm
[PE2-Vlan-interface12] quit
```

5. Configure the MVPN for the VPN instance:

On PE 1, create service loopback group 1 and specify the multicast tunnel service.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE1] interface ten-gigabitethernet 1/0/4
[PE1-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE1-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

On PE 2, create service loopback group 1 and specify the multicast tunnel service.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE2] interface ten-gigabitethernet 1/0/4
[PE2-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE2-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

Verifying the configuration

Verify the establishment of the default-MDT for the public network on PEs and P. The following example shows PIM routing table for the public network on P.

```
[P] display pim routing-table
 Total 1 (*, G) entries; 2 (S, G) entries

 (*, 239.1.1.1)
    RP: 3.3.3.3 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 02:54:43
    Upstream interface: Register
       Upstream neighbor: NULL
       RPF prime neighbor: NULL
```

```
    Downstream interface(s) information:
    Total number of downstreams: 2
       1: Vlan-interface2
          Protocol: pim-sm, UpTime: 02:54:43, Expires: -
       2: Vlan-interface3
          Protocol: pim-sm, UpTime: 02:33:57, Expires: -

 (1.1.1.1, 239.1.1.1)
    RP: 3.3.3.3 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 01:57:13
    Upstream interface: Vlan-interface2
       Upstream neighbor: 192.168.1.2
       RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information: None

(1.1.1.2, 239.1.1.1)
    RP: 3.3.3.3 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 01:57:13
    Upstream interface: Vlan-interface3
       Upstream neighbor: 192.168.2.2
       RPF prime neighbor: 192.168.2.2
    Downstream interface(s) information: None
```

The output shows that an RPT for (*, 239.1.1.1), an SPT for (1.1.1.1, 239.1.1.1), and an SPT for (1.1.1.2, 239.1.1.1) have been established on the public network. The RPT and SPTs constitute the default-MDT for the public network.

Configuration files

- PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 import-extcommunity
 vpn-target 111:1 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 2
#
vlan 11
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface Vlan-interface2
```

```
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface11
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- PE 2:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 111:1 import-extcommunity
 vpn-target 111:1 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 3
#
vlan 12
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface Vlan-interface3
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface12
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
```

```
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- P:

```
#
vlan 2 to 3
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface Vlan-interface2
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface3
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 3.3.3.3
 c-rp 3.3.3.3
#
```

- CE a1:

```
#
vlan 10 to 11
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface Vlan-interface10
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
```

```
interface Vlan-interface11
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2:

```
#
vlan 12
#
vlan 20
#
interface Vlan-interface12
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface20
 ip address 10.11.4.1 255.255.255.0
 igmp enable
#
multicast routing
#
```

Example: Configuring inter-AS option A MDT-based MVPN

Network configuration

As shown in Figure 2:

- Customer A has two branches that separately connect to AS 100 and AS 200.
- ASBR-PE 1 and ASBR-PE 2 are interconnected by using the inter-AS option A solution.
- PIM-SM runs within the two branches.
- The multicast source and the receiver host are in different branches.

Configure inter-AS option A MDT-based MVPN so that the receiver host can receive the multicast data from the source.

Figure 2 Network diagram

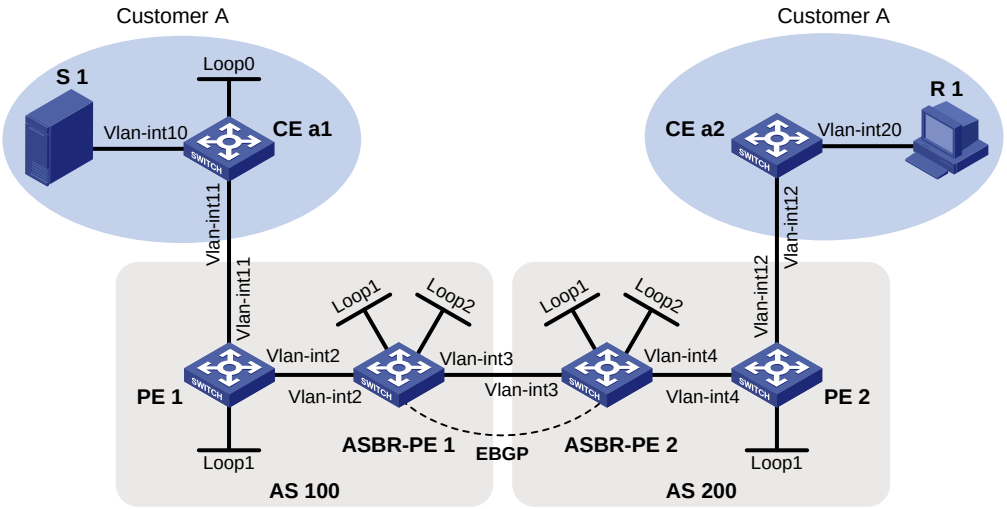


Table 2 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.11.3.2/24	R 1	—	10.11.4.2/24
PE 1	Vlan-int2	192.168.1.2/24	ASBR-PE 2	Vlan-int4	192.168.3.2/24
PE 1	Vlan-int11	10.11.1.1/24	ASBR-PE 2	Vlan-int3	192.168.2.2/24
PE 1	Loop1	1.1.1.1/32	ASBR-PE 2	Loop1	1.1.1.3/32
ASBR-PE 1	Vlan-int2	192.168.1.1/24	ASBR-PE 2	Loop2	22.22.22.22/32
ASBR-PE 1	Vlan-int3	192.168.2.1/24	PE 2	Vlan-int4	192.168.3.1/24
ASBR-PE 1	Loop1	1.1.1.2/32	PE 2	Vlan-int12	10.11.2.1/24
ASBR-PE 1	Loop2	11.11.11.11/32	PE 2	Loop1	1.1.1.4/32
CE a1	Vlan-int10	10.11.3.1/24	CE a2	Vlan-int20	10.11.4.1/24
CE a1	Vlan-int11	10.11.1.2/24	CE a2	Vlan-int12	10.11.2.2/24
CE a1	Loopback 0	2.2.2.2/32			

Analysis

To meet the network requirement, you must create a separate MDT-based MVPN for each AS.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported

Hardware	Software version
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure the inter-AS option A MDT-based MVPN, follow these restrictions and guidelines:

- You must enable the same PIM mode for all interfaces that belong to the same VPN instance (including the interface associated with the VPN instance). You may enable different PIM modes for the public network in different ASs.
- You must specify the same default-group for the same VPN instance in the same AS. You may specify different default-groups for the same VPN instance in different ASs.

Procedures

1. Assign an IP address and subnet mask to each interface on CE a1, as shown in Table 2.

```
<CEa1> system-view
```

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.11.3.1 24
[CEa1-Vlan-interface10] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.11.1.2 24
[CEa1-Vlan-interface11] quit
```

Configure PE 1, ASBR-PE 1, ASBR-PE2, PE 2, and CE a2 in the same way CE a1 is configured. (Details not shown.)

2. Configure a unicast routing protocol and MPLS L3VPN inter-AS option A on all devices so that all devices in the ASs are interoperable at the network layer. (Details not shown)

For more information about configuring basic MPLS VPN, see *MPLS Configuration Guide*.

3. Enable IP multicast routing on the public network, and enable PIM-SM on the public network interfaces (including Loopback interfaces):

On PE 1, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

On ASBR-PE 1, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface vlan-interface 2
[ASBR-PE1-Vlan-interface2] pim sm
[ASBR-PE1-Vlan-interface2] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
[ASBR-PE1-LoopBack1] quit
[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11
[ASBR-PE1-pim] c-rp 11.11.11.11
[ASBR-PE1-pim] quit
```

On PE 2, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface vlan-interface 4
[PE2-Vlan-interface4] pim sm
```

```
[PE2-Vlan-interface4] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

On ASBR-PE 2, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[ASBR-PE2] multicast routing
[ASBR-PE2-mrib] quit
[ASBR-PE2] interface vlan-interface 4
[ASBR-PE2-Vlan-interface4] pim sm
[ASBR-PE2-Vlan-interface4] quit
[ASBR-PE2] interface loopback 1
[ASBR-PE2-LoopBack1] pim sm
[ASBR-PE2-LoopBack1] quit
[ASBR-PE2] interface loopback 2
[ASBR-PE2-LoopBack2] pim sm
[ASBR-PE2-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[ASBR-PE2] pim
[ASBR-PE2-pim] c-bsr 22.22.22.22
[ASBR-PE2-pim] c-rp 22.22.22.22
[ASBR-PE2-pim] quit
```

4. Enable IP multicast routing for the VPN instances, enable PIM-SM on the VPN instance interfaces, and enable IGMP on the interfaces that have receiver hosts attached:

NOTE:

The route targets for the same VPN instance on the ASBRs and PEs within the same AS must match. Those within different ASs do not need to match.

On CE a1, enable IP multicast routing, enable PIM-SM on each interface.

```
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
```

Configure Loopback 0 as a C-BSR and a C-RP.

```
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

On CE a2, enable IP multicast routing, enable PIM-SM on VLAN-interface 12, and enable IGMP on VLAN-interface 20.

```
[CEa2] multicast routing
```

```
[CEa2-mrib] quit
[CEa2] interface vlan-interface 12
[CEa2-Vlan-interface12] pim sm
[CEa2-Vlan-interface12] quit
[CEa2] interface vlan-interface 20
[CEa2-Vlan-interface20] igmp enable
[CEa2-Vlan-interface20] quit
```

On PE 1, create a VPN instance named **customerA**.

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 100:1
[PE1-vpn-instance-customerA] vpn-target 100:1 both
[PE1-vpn-instance-customerA] quit
```

Associate VLAN-interface 11 with VPN instance **customerA**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance customerA
[PE1-Vlan-interface11] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 11.

```
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

On PE 2, create a VPN instance named **customerA**.

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 12:12
[PE2-vpn-instance-customerA] vpn-target 3:3 import-extcommunity
[PE2-vpn-instance-customerA] vpn-target 3:3 export-extcommunity
[PE2-vpn-instance] quit
```

Associate VLAN-interface 12 with VPN instance **customerA**.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] ip binding vpn-instance customerA
[PE2-Vlan-interface12] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 12.

```
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] pim sm
[PE2-Vlan-interface12] quit
```

On ASBR-PE 1, create a VPN instance named **customerA**.

```
[ASBR-PE1] ip vpn-instance customerA
[ASBR-PE1-vpn-instance-customerA] route-distinguisher 100:1
[ASBR-PE1-vpn-instance-customerA] vpn-target 100:1 both
[ASBR-PE1-vpn-instance-customerA] quit
```

Associate VLAN-interface 3 with VPN instance **customerA**.

```
[ASBR-PE1] interface vlan-interface 3
[ASBR-PE1-Vlan-interface3] ip binding vpn-instance customerA
```

```
[ASBR-PE1-Vlan-interface3] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 3.

```
[ASBR-PE1] multicast routing vpn-instance customerA
[ASBR-PE1-mrib-customerA] quit
[ASBR-PE1] interface vlan-interface 3
[ASBR-PE1-Vlan-interface3] pim sm
[ASBR-PE1-Vlan-interface3] quit
```

On ASBR-PE 2, create a VPN instance named **customerA**.

```
[ASBR-PE2] ip vpn-instance customerA
[ASBR-PE2-vpn-vpn-customerA] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-customerA] vpn-target 200:1 both
[ASBR-PE2-vpn-vpn-customerA] quit
```

Associate VLAN-interface 3 with VPN instance **customerA**.

```
[ASBR-PE2] interface vlan-interface 3
[ASBR-PE2-Vlan-interface3] ip binding vpn-instance customerA
[ASBR-PE2-Vlan-interface3] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 3.

```
[ASBR-PE2] multicast routing vpn-instance customerA
[ASBR-PE2-mrib-customerA] quit
[ASBR-PE2] interface vlan-interface 3
[ASBR-PE2-Vlan-interface3] pim sm
[ASBR-PE2-Vlan-interface3] quit
```

5. Configure the MDT-based MVPN for the VPN instance:

On PE 1, create service loopback group 1 and specify the multicast tunnel service.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE1] interface ten-gigabitethernet 1/0/4
[PE1-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE1-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-customerA-ipv4] quit
[PE1-mvpn-customerA] quit
```

On ASBR-PE 1, create service loopback group 1 and specify the multicast tunnel service.

```
[ASBR-PE1] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[ASBR-PE1] interface ten-gigabitethernet 1/0/4
[ASBR-PE1-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[ASBR-PE1-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[ASBR-PE1] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[ASBR-PE1-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[ASBR-PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE1-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE1-mvpn-customerA-ipv4] quit
[ASBR-PE1-mvpn-customerA] quit
```

On PE 2, create service loopback group 1 and specify the multicast tunnel service.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE2] interface ten-gigabitethernet 1/0/4
[PE2-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE2-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

On ASBR-PE 2, create service loopback group 1 and specify the multicast tunnel service.

```
[ASBR-PE2] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[ASBR-PE2] interface ten-gigabitethernet 1/0/4
[ASBR-PE2-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[ASBR-PE2-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[ASBR-PE2] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[ASBR-PE2-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[ASBR-PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[ASBR-PE2-mvpn-customerA-ipv4] source loopback 1
[ASBR-PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[ASBR-PE2-mvpn-customerA-ipv4] quit
[ASBR-PE2-mvpn-customerA] quit
```

Verifying the configuration

Verify that the default-MDT has been established on the public network in each AS on PEs and ASBR-PEs. The following example shows PIM routing table for the public network on ASBR-PE 1.

```
[ASBR-PE1]display pim routing-table
 Total 1 (*, G) entries; 1 (S, G) entries

 (*, 239.1.1.1)
    RP: 11.11.11.11 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 02:54:43
    Upstream interface: Register
       Upstream neighbor: NULL
       RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
       1: Vlan-interface2
          Protocol: pim-sm, UpTime: 02:54:43, Expires: -

 (1.1.1.1, 239.1.1.1)
    RP: 11.11.11.11 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 01:57:13
    Upstream interface: Vlan-interface2
       Upstream neighbor: 192.168.1.2
       RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information: None
```

The output shows that an RPT for (*, 239.1.1.1) and an SPT for (1.1.1.1, 239.1.1.1) have been established on the public network. The RPT and SPT constitute the default-MDT for the public network.

Configuration files

- PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 2
#
vlan 11
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
```

```
 pim sm
#
interface Vlan-interface2
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface11
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- PE 2:

```
#
ip vpn-instance customerA
 route-distinguisher 200:2
 vpn-target 200:2 import-extcommunity
 vpn-target 200:2 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 4
#
vlan 12
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface Vlan-interface4
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface12
 ip binding vpn-instance customerA
```

```
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- ASBR-PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 2 to 3
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface Vlan-interface2
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface3
 ip binding vpn-instance customerA
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
```

```
#
multicast routing
#
multicast routing vpn-instance customerA
#
pim
 c-bsr 11.11.11.11
 c-rp 11.11.11.11
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- ASBR-PE 2:

```
#
ip vpn-instance customerA
 route-distinguisher 200:1
 vpn-target 200:1 import-extcommunity
 vpn-target 200:1 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 3 to 4
#
interface LoopBack1
 ip address 1.1.1.3 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 22.22.22.22 255.255.255.255
 pim sm
#
interface Vlan-interface3
 ip binding vpn-instance customerA
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface4
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
```

```
#
multicast routing vpn-instance customerA
#
pim
 c-bsr 22.22.22.22
 c-rp 22.22.22.22
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- CE a1:

```
#
vlan 10 to 11
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface Vlan-interface10
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface11
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2:

```
#
vlan 12
#
vlan 20
#
interface Vlan-interface12
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface20
 ip address 10.11.4.1 255.255.255.0
 igmp enable
```

```
#
multicast routing
#
```

Example: Configuring inter-AS option C MDT-based MVPN

Network configuration

As shown in Figure 3:

- Customer A has two branches that separately connect to AS 100 and AS 200.
- ASBR-PE 1 and ASBR-PE 2 are interconnected by using the inter-AS option C solution.
- PIM-SM runs within the two branches.
- The multicast source and the receiver host are in different branches.

Configure inter-AS option C MDT-based MVPN so that the receiver host can receive the multicast data from the source.

Figure 3 Network diagram

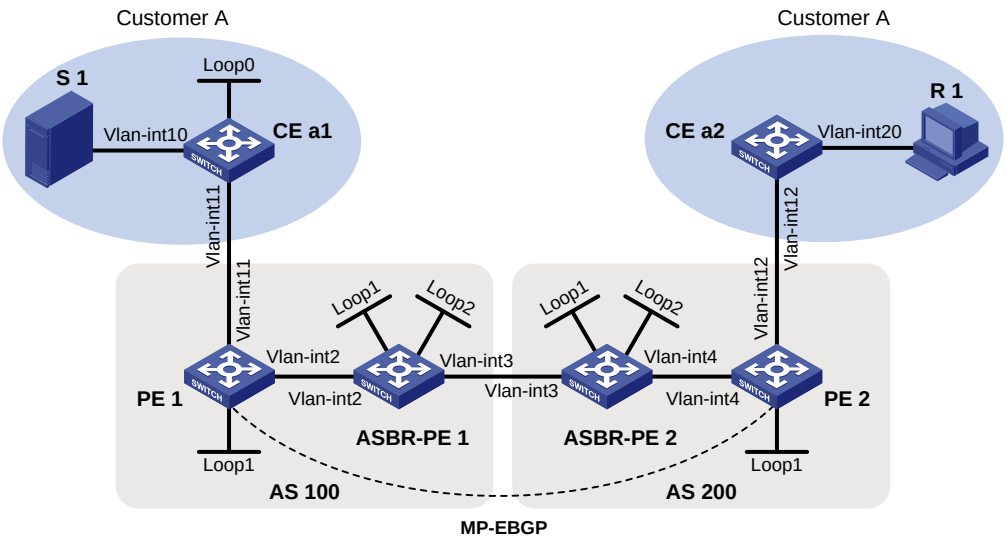


Table 3 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.11.3.2/24	R 1	—	10.11.4.2/24
PE 1	Vlan-int2	192.168.1.2/24	ASBR-PE2	Vlan-int4	192.168.3.2/24
PE 1	Vlan-int11	10.11.1.1/24	ASBR-PE2	Vlan-int3	192.168.2.2/24
PE 1	Loop1	1.1.1.1/32	ASBR-PE2	Loop1	1.1.1.3/32
ASBR-PE1	Vlan-int2	192.168.1.1/24	ASBR-PE2	Loop2	22.22.22.22/32
ASBR-PE1	Vlan-int3	192.168.2.1/24	PE 2	Vlan-int4	192.168.3.1/24
ASBR-PE1	Loop1	1.1.1.2/32	PE 2	Vlan-int12	10.11.2.1/24
ASBR-PE1	Loop2	11.11.11.11/32	PE 2	Loop1	1.1.1.4/32

Device	Interface	IP address	Device	Interface	IP address
CE a1	Vlan-int10	10.11.3.1/24	CE a2	Vlan-int20	10.11.4.1/24
CE a1	Vlan-int11	10.11.1.2/24	CE a2	Vlan-int12	10.11.2.2/24
CE a1	Loop0	2.2.2.2/32			

Analysis

To meet the network requirement, you must perform the following tasks:

- Create the same MDT-based MVPN for each AS.
- Establish MSDP peering relationships between the RPs in the ASs to share the multicast source information in different PIM-SM domains.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported

Hardware	Software version
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported

Hardware	Software version
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

1. Assign an IP address and subnet mask to each interface on CE a1, as shown in Table 3.

```
<CEa1> system-view
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.11.3.1 24
[CEa1-Vlan-interface10] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] ip address 2.2.2.2 32
[CEa1-LoopBack0] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.11.1.2 24
[CEa1-Vlan-interface11] quit
```

   # Configure PE 1, ASBR-PE 1, ASBR-PE 2, PE 2, and CE a2 in the same way CE a1 is configured. (Details not shown.)

2. Configure a unicast routing protocol and basic MPLS VPN on all devices so that all devices are interoperable at the network layer. (Details not shown)

   For more information about configuring basic MPLS VPN, see *MPLS Configuration Guide*.

3. Enable IP multicast routing on the public network in each AS, enable PIM-SM on the public network interfaces (including Loopback interfaces), and configure PIM-SM domain boarders:

   # On PE 1, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE1] multicast routing
[PE1-mrib] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] quit
[PE1] interface loopback 1
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

   # On ASBR-PE 1, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[ASBR-PE1] multicast routing
[ASBR-PE1-mrib] quit
[ASBR-PE1] interface vlan-interface 2
[ASBR-PE1-Vlan-interface2] pim sm
[ASBR-PE1-Vlan-interface2] quit
[ASBR-PE1] interface vlan-interface 3
[ASBR-PE1-Vlan-interface3] pim sm
```

```
[ASBR-PE1-Vlan-interface3] quit
[ASBR-PE1] interface loopback 1
[ASBR-PE1-LoopBack1] pim sm
[ASBR-PE1-LoopBack1] quit
[ASBR-PE1] interface loopback 2
[ASBR-PE1-LoopBack2] pim sm
[ASBR-PE1-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[ASBR-PE1] pim
[ASBR-PE1-pim] c-bsr 11.11.11.11
[ASBR-PE1-pim] c-rp 11.11.11.11
[ASBR-PE1-pim] quit
```

Configure VLAN-interface 3 as a PIM-SM domain boarder.

```
[ASBR-PE1] interface vlan-interface 3
[ASBR-PE1-Vlan-interface3] pim bsr-boundary
[ASBR-PE1-Vlan-interface3] quit
```

On PE 2, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[PE2] multicast routing
[PE2-mrib] quit
[PE2] interface vlan-interface 4
[PE2-Vlan-interface4] pim sm
[PE2-Vlan-interface4] quit
[PE2] interface loopback 1
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

On ASBR-PE 2, enable IP multicast routing, and enable PIM-SM on the public network interfaces.

```
[ASBR-PE2] multicast routing
[ASBR-PE2-mrib] quit
[ASBR-PE2] interface vlan-interface 3
[ASBR-PE2-Vlan-interface3] pim sm
[ASBR-PE2-Vlan-interface3] quit
[ASBR-PE2] interface vlan-interface 4
[ASBR-PE2-Vlan-interface4] pim sm
[ASBR-PE2-Vlan-interface4] quit
[ASBR-PE2] interface loopback 1
[ASBR-PE2-LoopBack1] pim sm
[ASBR-PE2-LoopBack1] quit
[ASBR-PE2] interface loopback 2
[ASBR-PE2-LoopBack2] pim sm
[ASBR-PE2-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[ASBR-PE2] pim
[ASBR-PE2-pim] c-bsr 22.22.22.22
[ASBR-PE2-pim] c-rp 22.22.22.22
[ASBR-PE2-pim] quit
```

Configure VLAN-interface 3 as a PIM-SM domain boarder.

```
[ASBR-PE2] interface vlan-interface 3
```

```
[ASBR-PE2-Vlan-interface3] pim bsr-boundary
[ASBR-PE2-Vlan-interface3] quit
```

4. Establish MSDP peering relationships between the RPs on the public network in the ASs:

   # On ASBR-PE 1, specify an MSDP peer.

```
[ASBR-PE1] msdp
[ASBR-PE1-msdp] encap-data-enable
[ASBR-PE1-msdp] peer 192.168.2.2 connect-interface vlan-interface 3
```

   # On ASBR-PE 2, specify an MSDP peer.

```
[ASBR-PE2] msdp
[ASBR-PE2-msdp] encap-data-enable
[ASBR-PE2-msdp] peer 192.168.2.1 connect-interface vlan-interface 3
```

5. Enable IP multicast routing for the VPN instance, enable PIM-SM on the private network interfaces, and enable IGMP on the interfaces that have receiver hosts attached:

   NOTE:

   The route targets for the same VPN instance on the ASBRs and PEs within the same AS must match. Those within different ASs do not need to match.

   # On CE a1, enable IP multicast routing, and enable PIM-SM on each interface.

```
[CEa1] multicast routing
[CEa1-mrib] quit
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
[CEa1] interface loopback 0
[CEa1-LoopBack0] pim sm
[CEa1-LoopBack0] quit
```

   # Configure Loopback 0 as a C-BSR and a C-RP.

```
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

   # On CE a2, enable IP multicast routing, enable PIM-SM on VLAN-interface 12, and enable IGMP on VLAN-interface 20.

```
[CEa2] multicast routing
[CEa2-mrib] quit
[CEa2] interface vlan-interface 12
[CEa2-Vlan-interface12] pim sm
[CEa2-Vlan-interface12] quit
[CEa2] interface vlan-interface 20
[CEa2-Vlan-interface20] igmp enable
[CEa2-Vlan-interface20] quit
```

   # On PE 1, create a VPN instance named **customerA**.

```
[PE1] ip vpn-instance customerA
[PE1-vpn-instance-customerA] route-distinguisher 11:11
[PE1-vpn-instance-customerA] vpn-target 3:3 import-extcommunity
```

```
[PE1-vpn-instance-customerA] vpn-target 3:3 export-extcommunity
[PE1-vpn-instance-customerA] quit
```

Associate VLAN-interface 11 with VPN instance **customerA**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance customerA
[PE1-Vlan-interface11] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 11.

```
[PE1] multicast routing vpn-instance customerA
[PE1-mrib-customerA] quit
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

On PE 2, create a VPN instance named **customerA**.

```
[PE2] ip vpn-instance customerA
[PE2-vpn-instance-customerA] route-distinguisher 12:12
[PE2-vpn-instance-customerA] vpn-target 3:3 import-extcommunity
[PE2-vpn-instance-customerA] vpn-target 3:3 export-extcommunity
[PE2-vpn-instance] quit
```

Associate VLAN-interface 12 with VPN instance **customerA**.

```
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] ip binding vpn-instance customerA
[PE2-Vlan-interface12] quit
```

Enable IP multicast routing for VPN instance **customerA**, and enable PIM-SM on VLAN-interface 12.

```
[PE2] multicast routing vpn-instance customerA
[PE2-mrib-customerA] quit
[PE2] interface vlan-interface 12
[PE2-Vlan-interface12] pim sm
[PE2-Vlan-interface12] quit
```

6. Create the same MDT-based MVPN for the ASs, and specify the default-group, MVPN source interface, and data-group for the MVPN:

On PE 1, create service loopback group 1 and specify the multicast tunnel service.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE1] interface ten-gigabitethernet 1/0/4
[PE1-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE1] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE1-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE1-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE1-mvpn-customerA-ipv4] source loopback 1
[PE1-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
```

```
[PE1-mvpn-customerA] quit
```

On PE 2, create service loopback group 1 and specify the multicast tunnel service.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

Assign Ten-GigabitEthernet 1/0/4 to service loopback group 1.

```
[PE2] interface ten-gigabitethernet 1/0/4
[PE2-Ten-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-Ten-GigabitEthernet1/0/4] quit
```

Create an MDT-based MVPN for VPN instance **customerA**.

```
[PE2] multicast-vpn vpn-instance customerA mode mdt
```

Create an MVPN IPv4 address family for VPN instance **customerA**.

```
[PE2-mvpn-customerA] address-family ipv4
```

Specify the default group, MVPN source interface, and data group range for VPN instance **customerA**.

```
[PE2-mvpn-customerA-ipv4] default-group 239.1.1.1
[PE2-mvpn-customerA-ipv4] source loopback 1
[PE2-mvpn-customerA-ipv4] data-group 225.2.2.0 28
[PE2-mvpn-customerA-ipv4] quit
[PE2-mvpn-customerA] quit
```

Verifying the configuration

Verify that the default-MDT has been established on the public network in each AS on PEs and ASBR-PEs. The following example shows PIM routing table for the public network on ASBR-PE 1.

```
[ASBR-PE1]display pim routing-table
 Total 1 (*, G) entries; 2 (S, G) entries

 (*, 239.1.1.1)
    RP: 3.3.3.3 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 02:54:43
    Upstream interface: Register
       Upstream neighbor: NULL
       RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
       1: Vlan-interface2
           Protocol: pim-sm, UpTime: 02:54:43, Expires: -

 (1.1.1.1, 239.1.1.1)
    RP: 3.3.3.3 (local)
    Protocol: pim-sm, Flag: SPT LOC ACT
    UpTime: 01:57:13
    Upstream interface: Vlan-interface2
       Upstream neighbor: 192.168.1.2
       RPF prime neighbor: 192.168.1.2
    Downstream interface(s) information: None

(1.1.1.4, 239.1.1.1)
```

```
RP: 3.3.3.3 (local)
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 01:57:13
Upstream interface: Vlan-interface3
   Upstream neighbor: 192.168.2.2
   RPF prime neighbor: 192.168.2.2
Downstream interface(s) information: None
```

The output shows that an RPT for (*, 239.1.1.1), an SPT for (1.1.1.1, 239.1.1.1), and an SPT for (1.1.1.4, 239.1.1.1) have been established on the public network. The RPT and SPTs constitute the default-MDT for the public network.

Configuration files

- PE 1:

```
#
ip vpn-instance customerA
 route-distinguisher 11:11
 vpn-target 3:3 import-extcommunity
 vpn-target 3:3 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 2
#
vlan 11
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface Vlan-interface2
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface11
 ip binding vpn-instance customerA
 ip address 10.11.1.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
```

```
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- PE 2:

```
#
ip vpn-instance customerA
 route-distinguisher 12:12
 vpn-target 3:3 import-extcommunity
 vpn-target 3:3 export-extcommunity
#
 service-loopback group 1 type multicast-tunnel
#
vlan 4
#
vlan 12
#
interface LoopBack1
 ip address 1.1.1.4 255.255.255.255
 pim sm
#
interface Vlan-interface4
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface12
 ip binding vpn-instance customerA
 ip address 10.11.2.1 255.255.255.0
 pim sm
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port service-loopback group 1
#
multicast routing
#
multicast routing vpn-instance customerA
#
multicast-vpn vpn-instance customerA mode mdt
 address-family ipv4
  source LoopBack1
  default-group 239.1.1.1
  data-group 225.2.2.0 255.255.255.240
#
```

- ASBR-PE 1:

```
#
vlan 2 to 3
```

```
#
interface LoopBack1
 ip address 1.1.1.2 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 11.11.11.11 255.255.255.255
 pim sm
#
interface Vlan-interface2
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface3
 ip address 192.168.2.1 255.255.255.0
 pim sm
 pim bsr-boundary
#
multicast routing
#
pim
 c-bsr 11.11.11.11
 c-rp 11.11.11.11
#
msdp
 encap-data-enable
 peer 192.168.2.2 connect-interface Vlan-interface3
#
```

- ASBR-PE 2:

```
#
vlan 3 to 4
#
interface LoopBack1
 ip address 1.1.1.3 255.255.255.255
 pim sm
#
interface LoopBack2
 ip address 22.22.22.22 255.255.255.255
 pim sm
#
interface Vlan-interface3
 ip address 192.168.2.2 255.255.255.0
 pim sm
 pim bsr-boundary
#
interface Vlan-interface4
 ip address 192.168.3.2 255.255.255.0
 pim sm
```

```
#
multicast routing
#
pim
 c-bsr 22.22.22.22
 c-rp 22.22.22.22
#
msdp
 encap-data-enable
 peer 192.168.2.1 connect-interface Vlan-interface3
#
```

- CE a1:

```
#
vlan 10 to 11
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface Vlan-interface10
 ip address 10.11.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface11
 ip address 10.11.1.2 255.255.255.0
 pim sm
#
multicast routing
#
pim
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
```

- CE a2:

```
#
vlan 12
#
vlan 20
#
interface Vlan-interface12
 ip address 10.11.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface20
 ip address 10.11.4.1 255.255.255.0
 igmp enable
#
multicast routing
```

#

Contents

Introduction

This document provides MPLS TE configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MPLS TE.

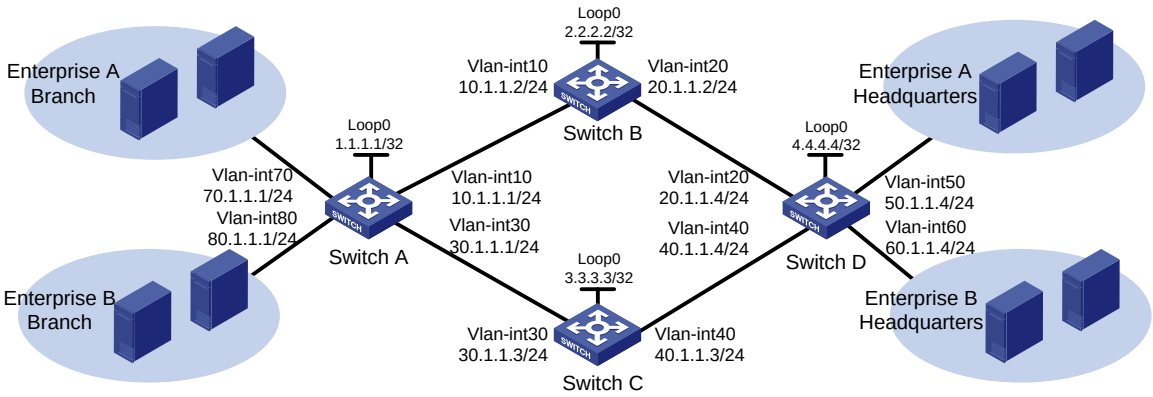
Example: Establishing MPLS TE tunnels with RSVP-TE

Network configuration

As shown in Figure 1, use RSVP-TE to establish two MPLS TE tunnels between Switch A and Switch D. The MPLS TE tunnel for Enterprise A requires a bandwidth of 20000 kbps. The MPLS TE tunnel for Enterprise B requires a bandwidth of 30000 kbps.

The maximum bandwidth of the link that each tunnel traverses is 50000 kbps and the maximum reservable bandwidth is 40000 kbps.

Figure 1 Network diagram



Analysis

To establish MPLS TE tunnels through RSVP-TE, you must perform the following tasks:

- Enable MPLS, MPLS TE, and RSVP-TE on nodes that the MPLS TE tunnels traverse.
- On each interface that the MPLS TE tunnels traverse, configure link TE attributes, including the maximum link bandwidth and the maximum reservable bandwidth.
- On each node that the MPLS TE tunnels traverse, configure the IGP TE extension to advertise the link TE attributes, which generates a TEDB on each node.

Based on the TEDB, CSPF calculates the shortest, TE constraints-compliant path to the tunnel destination. If you do not configure the IGP TE extension, the path is created based on IGP routing. The supported IGP TE extensions are OSPF TE and ISIS TE. This example uses OSPF TE.

- Create a tunnel interface on the ingress node of each MPLS TE tunnel, and perform the following tasks on the tunnel interface:
  - Specify the tunnel destination address.
  - Specify the tunnel bandwidth as required (20000 kbps for Enterprise A and 30000 kbps for Enterprise B).
  - Specify the MPLS TE signaling protocol as RSVP-TE.

    RSVP-TE advertises labels to establish CRLSPs and reserves bandwidth resources on each node along the calculated path.
- On the ingress node of each MPLS TE tunnel, configure static routing to direct traffic to the MPLS TE tunnel.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5850 switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported

Hardware	Software version
S5500V3-24P-SI S5500V3-48P-SI	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported

Hardware	Software version
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

To generate a TEDB on each node that the MPLS TE tunnels traverse, you must configure the IGP TE extension to advertise the link TE attributes. If you do not configure the IGP TE extension, the path is created based on IGP routing rather than CSPF..

Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI.

Procedures

1. Configure IP addresses for interfaces:

   # Configure IP addresses and masks for interfaces on Switch A, including the loopback interface, as shown in Figure 1.

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] port twenty-fivegige 1/0/1
[SwitchA-vlan10] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.1.1.1 24
[SwitchA-Vlan-interface10] quit
[SwitchA] vlan 30
[SwitchA-vlan30] port twenty-fivegige 1/0/2
[SwitchA-vlan30] quit
[SwitchA] interface vlan-interface 30
[SwitchA-Vlan-interface30] ip address 30.1.1.1 24
[SwitchA-Vlan-interface30] quit
[SwitchA] vlan 70
[SwitchA-vlan70] port twenty-fivegige 1/0/3
[SwitchA-vlan70] quit
[SwitchA] interface vlan-interface 70
[SwitchA-Vlan-interface70] ip address 70.1.1.1 24
[SwitchA-Vlan-interface70] quit
[SwitchA] vlan 80
[SwitchA-vlan80] port twenty-fivegige 1/0/4
[SwitchA-vlan80] quit
[SwitchA] interface vlan-interface 80
[SwitchA-Vlan-interface80] ip address 80.1.1.1 24
[SwitchA-Vlan-interface80] quit
[SwitchA] interface loopback 0
```

```
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] quit
```

Configure other devices in the same way that Switch A is configured. (Details not shown.)

2. Configure OSPF to ensure IP connectivity among the switches:

Configure Switch A.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure Switch B.

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure Switch D.

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Execute the **`display ip routing-table`** command on each switch to verify that the switches have learned the routes to one another, including the routes to the loopback interfaces. The following shows the output on Switch A.

```
[SwitchA] display ip routing-table

Destinations : 24        Routes : 24

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0           127.0.0.1       InLoop0
1.1.1.1/32          Direct  0    0           127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10   1           10.1.1.2        Vlan10
3.3.3.3/32          O_INTRA 10   1           30.1.1.3        Vlan30
```

```
4.4.4.4/32          O_INTRA 10   2           10.1.1.2        Vlan10
8.1.1.0/24          Direct  0    0           8.1.1.1         Tun2
8.1.1.0/32          Direct  0    0           8.1.1.1         Tun2
8.1.1.1/32          Direct  0    0           127.0.0.1       InLoop0
8.1.1.255/32        Direct  0    0           8.1.1.1         Tun2
10.1.1.0/24         Direct  0    0           10.1.1.1        Vlan10
10.1.1.0/32         Direct  0    0           10.1.1.1        Vlan10
10.1.1.1/32         Direct  0    0           127.0.0.1       InLoop0
10.1.1.255/32       Direct  0    0           10.1.1.1        Vlan10
20.1.1.0/24         O_INTRA 10   2           10.1.1.2        Vlan10
30.1.1.0/24         Direct  0    0           30.1.1.1        Vlan30
30.1.1.0/32         Direct  0    0           30.1.1.1        Vlan30
30.1.1.1/32         Direct  0    0           127.0.0.1       InLoop0
30.1.1.255/32       Direct  0    0           30.1.1.1        Vlan30
40.1.1.0/24         Static  1    0           0.0.0.0         Tun2
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

3. Configure an LSR ID, and enable MPLS, MPLS TE, and RSVP-TE:

Configure Switch A.

```
[SwitchA] mpls lsr-id 1.1.1.1
[SwitchA] mpls te
[SwitchA-te] quit
[SwitchA] rsvp
[SwitchA-rsvp] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] mpls enable
[SwitchA-Vlan-interface10] mpls te enable
[SwitchA-Vlan-interface10] rsvp enable
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 30
[SwitchA-Vlan-interface30] mpls enable
[SwitchA-Vlan-interface30] mpls te enable
[SwitchA-Vlan-interface30] rsvp enable
[SwitchA-Vlan-interface30] quit
```

Configure Switch B.

```
[SwitchB] mpls lsr-id 2.2.2.2
[SwitchB] mpls te
[SwitchB-te] quit
[SwitchB] rsvp
[SwitchB-rsvp] quit
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] mpls enable
[SwitchB-Vlan-interface10] mpls te enable
[SwitchB-Vlan-interface10] rsvp enable
[SwitchB-Vlan-interface10] quit
```

```
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] mpls enable
[SwitchB-Vlan-interface20] mpls te enable
[SwitchB-Vlan-interface20] rsvp enable
[SwitchB-Vlan-interface20] quit
```

Configure Switch C.

```
[SwitchC] mpls lsr-id 3.3.3.3
[SwitchC] mpls te
[SwitchC-te] quit
[SwitchC] rsvp
[SwitchC-rsvp] quit
[SwitchC] interface vlan-interface 30
[SwitchC-Vlan-interface30] mpls enable
[SwitchC-Vlan-interface30] mpls te enable
[SwitchC-Vlan-interface30] rsvp enable
[SwitchC-Vlan-interface30] quit
[SwitchC] interface vlan-interface 40
[SwitchC-Vlan-interface40] mpls enable
[SwitchC-Vlan-interface40] mpls te enable
[SwitchC-Vlan-interface40] rsvp enable
[SwitchC-Vlan-interface40] quit
```

Configure Switch D.

```
[SwitchD] mpls lsr-id 4.4.4.4
[SwitchD] mpls te
[SwitchD-te] quit
[SwitchD] rsvp
[SwitchD-rsvp] quit
[SwitchD] interface vlan-interface 20
[SwitchD-Vlan-interface20] mpls enable
[SwitchD-Vlan-interface20] mpls te enable
[SwitchD-Vlan-interface20] rsvp enable
[SwitchD-Vlan-interface20] quit
[SwitchD] interface vlan-interface 40
[SwitchD-Vlan-interface40] mpls enable
[SwitchD-Vlan-interface40] mpls te enable
[SwitchD-Vlan-interface40] rsvp enable
[SwitchD-Vlan-interface40] quit
```

4. Configure MPLS TE attributes of links:

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch A.

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] mpls te max-link-bandwidth 50000
[SwitchA-Vlan-interface10] mpls te max-reservable-bandwidth 40000
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 30
[SwitchA-Vlan-interface30] mpls te max-link-bandwidth 50000
[SwitchA-Vlan-interface30] mpls te max-reservable-bandwidth 40000
[SwitchA-Vlan-interface30] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch B.

```
[SwitchB] interface vlan-interface 10
[SwitchB-Vlan-interface10] mpls te max-link-bandwidth 50000
[SwitchB-Vlan-interface10] mpls te max-reservable-bandwidth 40000
[SwitchB-Vlan-interface10] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] mpls te max-link-bandwidth 50000
[SwitchB-Vlan-interface20] mpls te max-reservable-bandwidth 40000
[SwitchB-Vlan-interface20] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch C.

```
[SwitchC] interface vlan-interface 30
[SwitchC-Vlan-interface30] mpls te max-link-bandwidth 50000
[SwitchC-Vlan-interface30] mpls te max-reservable-bandwidth 40000
[SwitchC-Vlan-interface30] quit
[SwitchC] interface vlan-interface 40
[SwitchC-Vlan-interface40] mpls te max-link-bandwidth 50000
[SwitchC-Vlan-interface40] mpls te max-reservable-bandwidth 40000
[SwitchC-Vlan-interface40] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch D.

```
[SwitchD] interface vlan-interface 20
[SwitchD-Vlan-interface20] mpls te max-link-bandwidth 50000
[SwitchD-Vlan-interface20] mpls te max-reservable-bandwidth 40000
[SwitchD-Vlan-interface20] quit
[SwitchD] interface vlan-interface 40
[SwitchD-Vlan-interface40] mpls te max-link-bandwidth 50000
[SwitchD-Vlan-interface40] mpls te max-reservable-bandwidth 40000
[SwitchD-Vlan-interface40] quit
```

5. Configure OSPF TE to advertise link TE attributes:

Enable opaque LSA advertisement and reception on Switch A. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchA] ospf
[SwitchA-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch A.

```
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] mpls te enable
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch B. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchB] ospf
[SwitchB-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch B.

```
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] mpls te enable
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch C. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchC] ospf
```

```
[SwitchC-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch C.

```
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] mpls te enable
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch D. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchD] ospf
[SwitchD-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch D.

```
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] mpls te enable
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

6. Configure MPLS TE tunnels on Switch A:

Configure MPLS TE tunnel interface Tunnel 1 to forward traffic of Enterprise A.

```
[SwitchA] interface tunnel 1 mode mpls-te
[SwitchA-Tunnel1] ip address 7.1.1.1 255.255.255.0
```

Specify the tunnel destination address as the LSR ID of Switch D, use RSVP-TE to establish the tunnel, and assign 20000 kbps bandwidth to the tunnel.

```
[SwitchA-Tunnel1] destination 4.4.4.4
[SwitchA-Tunnel1] mpls te signaling rsvp-te
[SwitchA-Tunnel1] mpls te bandwidth 20000
```

Enable route recording for MPLS TE tunnel 1.

```
[SwitchA-Tunnel1] mpls te record-route
[SwitchA-Tunnel1] quit
```

Configure MPLS TE tunnel interface Tunnel 2 to forward traffic of Enterprise B.

```
[SwitchA] interface tunnel 2 mode mpls-te
[SwitchA-Tunnel2] ip address 8.1.1.1 255.255.255.0
```

Specify the tunnel destination address as the LSR ID of Switch D, use RSVP-TE to establish the tunnel, and assign 30000 kbps bandwidth to the tunnel.

```
[SwitchA-Tunnel2] destination 4.4.4.4
[SwitchA-Tunnel2] mpls te signaling rsvp-te
[SwitchA-Tunnel2] mpls te bandwidth 30000
```

Enable route recording for MPLS TE tunnel 2.

```
[SwitchA-Tunnel2] mpls te record-route
[SwitchA-Tunnel2] quit
```

7. Configure static routing on Switch A to direct traffic to the MPLS TE tunnels:

Configure a static route to direct traffic destined for 50.1.1.0/24 to MPLS TE tunnel interface Tunnel 1.

```
[SwitchA] ip route-static 50.1.1.0 24 tunnel 1 preference 1
```

Configure a static route to direct traffic destined for 60.1.1.0/24 to MPLS TE tunnel interface Tunnel 2.

```
[SwitchA] ip route-static 60.1.1.0 24 tunnel 2 preference 1
```

Verifying the configuration

Execute the **display interface tunnel brief** command on Switch A. The output shows that the two tunnel interfaces are up.

```
[SwitchA] display interface tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun1                 UP   UP       7.1.1.1
Tun2                 UP   UP       8.1.1.1
```

Execute the **display mpls te tunnel-interface** command on Switch A to display detailed information about the MPLS TE tunnels.

```
[SwitchA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 27415           Tunnel ID            : 1
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 20000 kbps
  Reserved Bandwidth   : 20000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -

Tunnel Name            : Tunnel 2
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
```

```
  LSP ID               : 27302           Tunnel ID            : 2
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : -
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Disabled
  FRR Flag             : Disabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

Execute the **`display ip routing-table`** command on Switch A. The output shows two static route entries with output interfaces of Tunnel 1 and Tunnel 2.

```
[SwitchA] display ip routing-table

Destinations : 28        Routes : 29

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
1.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10   1            10.1.1.2        Vlan10
3.3.3.3/32          O_INTRA 10   1            30.1.1.3        Vlan30
4.4.4.4/32          O_INTRA 10   2            10.1.1.2        Vlan10
                                              30.1.1.3        Vlan30
7.1.1.0/24          Direct  0    0            7.1.1.1         Tun1
7.1.1.0/32          Direct  0    0            7.1.1.1         Tun1
7.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
7.1.1.255/32        Direct  0    0            7.1.1.1         Tun1
8.1.1.0/24          Direct  0    0            8.1.1.1         Tun2
8.1.1.0/32          Direct  0    0            8.1.1.1         Tun2
8.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
8.1.1.255/32        Direct  0    0            8.1.1.1         Tun2
```

```
10.1.1.0/24         Direct  0    0           10.1.1.1        Vlan10
10.1.1.0/32         Direct  0    0           10.1.1.1        Vlan10
10.1.1.1/32         Direct  0    0           127.0.0.1       InLoop0
10.1.1.255/32       Direct  0    0           10.1.1.1        Vlan10
50.1.1.0/24         Static  1    0           0.0.0.0         Tun1
30.1.1.0/24         Direct  0    0           30.1.1.1        Vlan30
30.1.1.0/32         Direct  0    0           30.1.1.1        Vlan30
30.1.1.1/32         Direct  0    0           127.0.0.1       InLoop0
30.1.1.255/32       Direct  0    0           30.1.1.1        Vlan30
60.1.1.0/24         Static  1    0           0.0.0.0         Tun2
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

Execute the **`display rsvp lsp verbose`** command on Switch A to verify the following information:

- Tunnel 1 uses path Switch A—Switch B—Switch D, and has a bandwidth of 20000 kbps.
- Tunnel 2 uses path Switch A—Switch C—Switch D, and has a bandwidth of 30000 kbps.

```
[SwitchA] display rsvp lsp verbose
Tunnel name: SwitchA_t1
Destination: 4.4.4.4                    Source: 1.1.1.1
Tunnel ID: 1                            LSP ID: 27415
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1146
In-Interface: -                         Out-Interface: Vlan10
Nexthop: 10.1.1.2                       Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 20000 kbps             Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 6
  10.1.1.1/32         Flag: 0x00 (No FRR)
  10.1.1.2/32         Flag: 0x00 (No FRR)
  2.2.2.2/32          Flag: 0x20 (No FRR/Node-ID)
  20.1.1.2/32         Flag: 0x00 (No FRR)
  20.1.1.4/32         Flag: 0x00 (No FRR)
  4.4.4.4/32          Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None

Tunnel name: SwitchA_t2
Destination: 4.4.4.4                    Source: 1.1.1.1
Tunnel ID: 2                            LSP ID: 27302
LSR type: Ingress                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1150
In-Interface: -                         Out-Interface: Vlan30
Nexthop: 30.1.1.3                       Exclude-any: 0
```

```
Include-Any: 0                              Include-all: 0
Mean rate (CIR): 30000 kbps                 Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                              Class type: CT0
RRO number: 6
  30.1.1.1/32         Flag: 0x00 (No FRR)
  30.1.1.3/32         Flag: 0x00 (No FRR)
  3.3.3.3/32          Flag: 0x20 (No FRR/Node-ID)
  40.1.1.3/32         Flag: 0x00 (No FRR)
  40.1.1.4/32         Flag: 0x00 (No FRR)
  4.4.4.4/32          Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: None
```

Configuration files

- Switch A:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 1.1.1.1
#
vlan 10
#
vlan 30
#
vlan 70
#
vlan 80
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

```
interface Vlan-interface30
 ip address 30.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface70
 ip address 70.1.1.1 255.255.255.0
#
interface Vlan-interface80
 ip address 80.1.1.1 255.255.255.0
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 10
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 30
#
interface Twenty-FiveGigE1/0/3
 port link-mode bridge
 port access vlan 70
#
interface Twenty-FiveGigE1/0/4
 port link-mode bridge
 port access vlan 80
#
interface Tunnel1 mode mpls-te
 ip address 7.1.1.1 255.255.255.0
 mpls te bandwidth ct0 20000
 mpls te record-route
 destination 4.4.4.4
#
interface Tunnel2 mode mpls-te
 ip address 8.1.1.1 255.255.255.0
 mpls te bandwidth ct0 30000
 mpls te record-route
 destination 4.4.4.4
#
 ip route-static 50.1.1.0 24 Tunnel1 preference 1
 ip route-static 60.1.1.0 24 Tunnel2 preference 1
#
```

- Switch B:

```
#
ospf 1
```

```
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
vlan 10
#
vlan 20
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface20
 ip address 20.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 10
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 20
#
```

- Switch C:

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
```

```
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
vlan 30
#
vlan 40
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.0
#
interface Vlan-interface30
 ip address 30.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface40
 ip address 40.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 40
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 30
#
```

- Switch D:

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
```

```
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
vlan 20
#
vlan 40
#
vlan 50
#
vlan 60
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface20
 ip address 20.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface40
 ip address 40.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface50
 ip address 50.1.1.4 255.255.255.0
#
interface Vlan-interface60
 ip address 60.1.1.4 255.255.255.0
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 40
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 20
```

```
#
interface Twenty-FiveGigE1/0/3
 port link-mode bridge
 port access vlan 50
#
interface Twenty-FiveGigE1/0/4
 port link-mode bridge
 port access vlan 60
#
```

Example: Configuring MPLS TE forwarding adjacency

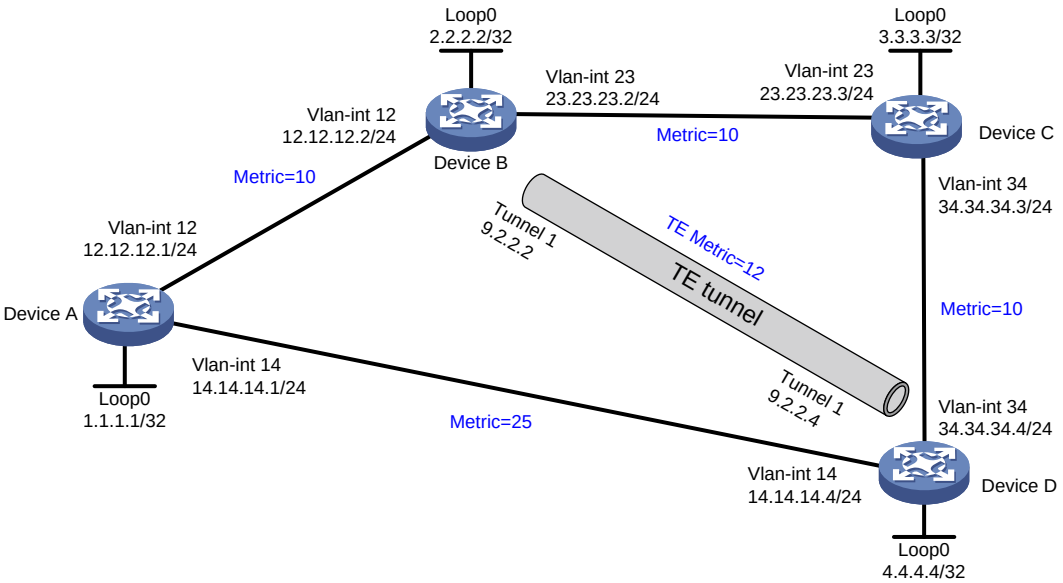
Network configuration

As shown in Figure 2, Device A, Device B, Device C, and Device D run OSPF.

Establish an MPLS TE tunnel from Device B to Device D that uses the path Device B—Device C—Device D, and configure MPLS TE forwarding adjacency for the tunnel.

Before the tunnel is established, traffic from Device A to Device D is forwarded through the direct link Device A—Device D. After the tunnel is established, the traffic is forwarded through the MPLS TE tunnel.

Figure 2 Network diagram



Analysis

- Enable MPLS TE on nodes and interfaces that the MPLS TE tunnels traverse.
- To make forwarding adjacency take effect, you must establish two MPLS TE tunnels in opposite directions between Device B and Device D, and enable forwarding adjacency on both devices.

- For the MPLS TE tunnel to use the path Device B—Device C—Device D, configure the path as the explicit path for the tunnel.
- For traffic from Device A to Device D to be forwarded through the MPLS TE tunnel, make sure the tunnel's metric is less than 15 (metric 25 minus 10). This example uses 12.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported

Hardware	Software version
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

By default, interfaces on the device are disabled (in **ADM** or **Administratively Down** state). To have an interface operate, you must use the **undo shutdown** command to enable that interface.

Procedures

1. Configure IP addresses for interfaces, configure basic OSPF, and set OSPF costs. (Details not shown.) For the configuration, see "Configuration files."
2. Enable MPLS TE on each node and interface that the MPLS TE tunnel traverses:

   # On Device B, configure an LSR ID, and enable MPLS, MPLS TE, and RSVP-TE.

```
<DeviceB> system-view
[DeviceB] mpls lsr-id 2.2.2.2
[DeviceB] mpls te
[DeviceB-te] quit
[DeviceB] rsvp
[DeviceB-rsvp] quit
[DeviceB] interface vlan-interface 23
[DeviceB-Vlan-interface23] mpls enable
[DeviceB-Vlan-interface23] mpls te enable
[DeviceB-Vlan-interface23] rsvp enable
[DeviceB-Vlan-interface23] quit
```

   # On Device C, configure an LSR ID, and enable MPLS, MPLS TE, and RSVP-TE.

```
<DeviceC> system-view
[DeviceC] mpls lsr-id 3.3.3.3
[DeviceC] mpls te
[DeviceC-te] quit
[DeviceC] rsvp
[DeviceC-rsvp] quit
[DeviceC] interface vlan-interface 23
[DeviceC-Vlan-interface23] mpls enable
[DeviceC-Vlan-interface23] mpls te enable
[DeviceC-Vlan-interface23] rsvp enable
[DeviceC-Vlan-interface23] quit
[DeviceC] interface vlan-interface 34
[DeviceC-Vlan-interface34] mpls enable
[DeviceC-Vlan-interface34] mpls te enable
[DeviceC-Vlan-interface34] rsvp enable
[DeviceC-Vlan-interface34] quit
```

   # On Device D, configure an LSR ID, and enable MPLS, MPLS TE, and RSVP-TE.

```
<DeviceD> system-view
[DeviceD] mpls lsr-id 4.4.4.4
[DeviceD] mpls te
[DeviceD-te] quit
[DeviceD] rsvp
[DeviceD-rsvp] quit
[DeviceD] interface vlan-interface 34
```

```
[DeviceD-Vlan-interface34] mpls enable
[DeviceD-Vlan-interface34] mpls te enable
[DeviceD-Vlan-interface34] rsvp enable
[DeviceD-Vlan-interface34] quit
```

3. Configure OSPF TE to advertise link TE attributes:

On Device B, enable opaque LSA advertisement and reception, and enable MPLS TE for OSPF area 0. By default, opaque LSA advertisement and reception are enabled.

```
[DeviceB] ospf
[DeviceB-ospf-1] opaque-capability enable
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] mpls te enable
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

On Device C, enable opaque LSA advertisement and reception, and enable MPLS TE for OSPF area 0. By default, opaque LSA advertisement and reception are enabled.

```
[DeviceC] ospf
[DeviceC-ospf-1] opaque-capability enable
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] mpls te enable
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

On Device D, enable opaque LSA advertisement and reception, and enable MPLS TE for OSPF area 0. By default, opaque LSA advertisement and reception are enabled.

```
[DeviceD] ospf
[DeviceD-ospf-1] opaque-capability enable
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] mpls te enable
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

4. Configure MPLS TE tunnels:

On Device B, configure MPLS TE tunnel interface Tunnel 1, and specify the tunnel destination address as the LSR ID of Device D.

```
[DeviceB] interface tunnel 1 mode mpls-te
[DeviceB-Tunnel1] ip address 9.2.2.2 255.255.255.0
[DeviceB-Tunnel1] destination 4.4.4.4
```

Configure MPLS TE to use RSVP-TE to establish the tunnel.

```
[DeviceB-Tunnel1] mpls te signaling rsvp-te
[DeviceB-Tunnel1] quit
```

Configure an explicit path named **tun1**.

```
[DeviceB] explicit-path tun1
[DeviceB-explicit-path-tun1] nexthop 23.23.23.3
[DeviceB-explicit-path-tun1] nexthop 34.34.34.4
[DeviceB-explicit-path-tun1]quit
```

Specify explicit path **tun1** for the tunnel.

```
[DeviceB] interface tunnel 1
[DeviceB–Tunnel1] mpls te path preference 1 explicit-path tun1
```

Enable forwarding adjacency for the tunnel.

```
[DeviceB-Tunnel1] mpls te igp advertise
```

Enable OSPF on tunnel interface Tunnel 1 and set the OSPF cost to 12 for the tunnel interface.

```
[DeviceB-Tunnel1] ospf 1 area 0
[DeviceB-Tunnel1] ospf cost 12
[DeviceB-Tunnel1] quit
```

On Device D, configure MPLS TE tunnel interface Tunnel 1, and specify the tunnel destination address as the LSR ID of Device B.

```
[DeviceD] interface tunnel 1 mode mpls-te
[DeviceD-Tunnel1] ip address 9.2.2.4  255.255.255.0
[DeviceD-Tunnel1] destination 2.2.2.2
```

Configure MPLS TE to use RSVP-TE to establish the tunnel.

```
[DeviceD-Tunnel1] mpls te signaling rsvp-te
[DeviceD-Tunnel1] quit
```

Configure an explicit path named **tun1**.

```
[DeviceD] explicit-path tun1
[DeviceD-explicit-path-tun1] nexthop 34.34.34.3
[DeviceD-explicit-path-tun1] nexthop 23.23.23.2
[DeviceD-explicit-path-tun1]quit
```

Specify explicit path **tun1** for the tunnel.

```
[DeviceD] interface tunnel 1
[DeviceD–Tunnel1] mpls te path preference 1 explicit-path tun1
```

Enable forwarding adjacency for the tunnel.

```
[DeviceD-Tunnel1] mpls te igp advertise
```

Enable OSPF on tunnel interface Tunnel 1 and set the OSPF cost to 12 for the tunnel interface.

```
[DeviceD-Tunnel1] ospf 1 area 0
[DeviceD-Tunnel1] ospf cost 12
[DeviceD-Tunnel1] quit
```

Verifying the configuration

Execute the **`display interface tunnel brief`** command on Device B and Device D. This example uses Device B. The output shows that Tunnel 1 is up.

```
[DeviceB] display interface tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun1                 UP   UP       9.2.2.2
```

Display routing table information on Device A. The output shows that the next hop of the route to Device D is Device B, and the cost is 22 (10 plus 12). The MPLS TE tunnel has been used during IGP route calculation.

```
[Device A] display ip routing-table

Destinations : 22        Routes : 22

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
```

```
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.2/32         O_INTRA 10  10          12.12.12.2      Vlan12
3.3.3.3/32         O_INTRA 10  20          12.12.12.2      Vlan12
4.4.4.4/32         O_INTRA 10  22          12.12.12.2      Vlan12
9.2.2.0/24         O_INTRA 10  22          12.12.12.2      Vlan12
10.1.0.3/32        Direct  0   0           127.0.0.1       InLoop0
12.12.12.0/24      Direct  0   0           12.12.12.1      Vlan12
12.12.12.0/32      Direct  0   0           12.12.12.1      Vlan12
12.12.12.1/32      Direct  0   0           127.0.0.1       InLoop0
12.12.12.255/32    Direct  0   0           12.12.12.1      Vlan12
14.14.14.0/24      Direct  0   0           14.14.14.1      Vlan14
14.14.14.0/32      Direct  0   0           14.14.14.1      Vlan14
14.14.14.1/32      Direct  0   0           127.0.0.1       InLoop0
14.14.14.255/32    Direct  0   0           14.14.14.1      Vlan14
23.23.23.0/24      O_INTRA 10  20          12.12.12.2      Vlan12
34.34.34.0/24      O_INTRA 10  30          12.12.12.2      Vlan12
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Configuration files

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 14.14.14.0 0.0.0.255
#
vlan 12
#
vlan 14
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.1 255.255.255.0
 ospf cost 10
#
interface Vlan-interface14
 ip address 14.14.14.1 255.255.255.0
 ospf cost 25
#
interface Twenty-FiveGigE1/0/1
```

```
 port link-mode bridge
 port access vlan 12
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 14
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 12.12.12.0 0.0.0.255
  network 23.23.23.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
vlan 12
#
vlan 23
#
mpls te
#
explicit-path tun1
 nexthop index 1 23.23.23.3 include strict
 nexthop index 101 34.34.34.4 include strict
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface12
 ip address 12.12.12.2 255.255.255.0
 ospf cost 10
#
interface Vlan-interface23
 ip address 23.23.23.2 255.255.255.0
 ospf cost 10
 mpls enable
 mpls te enable
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 12
#
```

```
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 23
#
interface Tunnel1 mode mpls-te
 ip address 9.2.2.2 255.255.255.0
 ospf cost 12
 ospf 1 area 0.0.0.0
 mpls te path preference 1 explicit-path tun1
 mpls te igp advertise
 destination 4.4.4.4
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 23.23.23.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
vlan 23
#
vlan 34
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface23
 ip address 23.23.23.3 255.255.255.0
 ospf cost 10
 mpls enable
 mpls te enable
 rsvp enable
#
interface Vlan-interface34
 ip address 34.34.34.3 255.255.255.0
 ospf cost 10
 mpls enable
 mpls te enable
 rsvp enable
#
```

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 34
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 23
#
```

- Device D:

```
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 14.14.14.0 0.0.0.255
  network 34.34.34.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
vlan 14
#
vlan 34
#
mpls te
#
explicit-path tun1
 nexthop index 1 34.34.34.3 include strict
 nexthop index 101 23.23.23.2 include strict
#
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface14
 ip address 14.14.14.4 255.255.255.0
 ospf cost 25
#
interface Vlan-interface34
 ip address 34.34.34.4 255.255.255.0
 ospf cost 10
 mpls enable
 mpls te enable
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 34
```

```
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 14
#
interface Tunnel1 mode mpls-te
ip address 9.2.2.4 255.255.255.0
 ospf cost 12
 ospf 1 area 0.0.0.0
 mpls te path preference 1 explicit-path tun1
 mpls te igp advertise
 destination 2.2.2.2
#
```

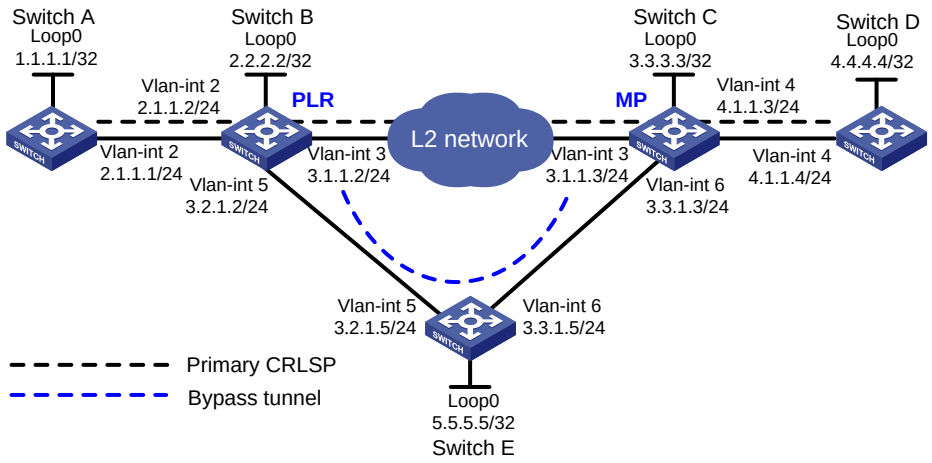
Example: Configuring MPLS TE FRR

Network configuration

As shown in Figure 3, on the primary CRLSP Switch A—Switch B—Switch C—Switch D, configure MPLS TE FRR to protect the link Switch B—Switch C. When the link between Switch B and Switch C fails, MPLS TE can immediately switch traffic to the bypass tunnel Switch B—Switch E—Switch C.

The primary CRLSP and the bypass tunnel each require a bandwidth of 30000 kbps. The maximum bandwidth of the link that each tunnel traverses is 50000 kbps and the maximum reservable bandwidth is 40000 kbps.

Figure 3 Network diagram



Analysis

To implement MPLS TE FRR, you must perform the following tasks:

- Enable MPLS, MPLS TE, and RSVP-TE on each switch for primary and bypass tunnel establishment.
- Configure explicit paths for the primary CRLSP and the bypass tunnel as required.
- Configure BFD for RSVP-TE on Switch B and Switch C for quick detection of the link failure.

BFD can immediately detect the failure of the protected link and notify RSVP-TE of the failure.

- Configure MPLS TE FRR on the ingress node of the primary CRLSP to ensure that traffic can be immediately switched to the bypass tunnel when BFD detects the failure of the protected link.
- If multiple bypass tunnels are specified for a primary CRLSP, MPLS TE selects an optimal bypass tunnel to protect the primary CRLSP. To make sure an optimal bypass tunnel is always selected, set the optimal bypass tunnel selection interval to 5 seconds on the PLR. The default interval for selecting an optimal bypass tunnel is 300 seconds.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported

Hardware	Software version
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported

Hardware	Software version
S5135S-EI switch series	Not supported

Restrictions and guidelines

When you configure MPLS TE FRR, follow these restrictions and guidelines:

- Before configuration, disable the spanning tree feature globally or map each VLAN to an MSTI.
- Only MPLS TE tunnels established through RSVP-TE support FRR.
- Do not configure both FRR and RSVP authentication on the same interface.
- Use bypass tunnels to protect only critical interfaces or links when bandwidth is insufficient. Bypass tunnels are pre-established and require extra bandwidth.
- Make sure the bandwidth assigned to the bypass tunnel is no less than the total bandwidth needed by all primary CRLSPs to be protected by the bypass tunnel. Otherwise, some primary CRLSPs might not be protected by the bypass tunnel.
- A bypass tunnel typically does not forward data when the primary CRLSP operates correctly. For a bypass tunnel to also forward data during tunnel protection, you must assign adequate bandwidth to the bypass tunnel.
- A bypass tunnel cannot be used for services such as VPN.
- You cannot configure FRR for a bypass tunnel. A bypass tunnel cannot act as a primary CRLSP.
- Make sure the protected node or interface is not on the bypass tunnel.
- After you associate a primary CRLSP that does not require bandwidth protection with a bypass tunnel that provides bandwidth protection, the primary CRLSP occupies the bandwidth that the bypass tunnel protects. The bandwidth is protected on a first-come-first-served basis. The primary CRLSP that needs bandwidth protection cannot preempt the one that does not need bandwidth protection.
- After an FRR, the primary CRLSP will be down if you modify the bandwidth that the bypass tunnel can protect and your modification results in one of the following:
  - The CT type changes.
  - The bypass tunnel cannot protect adequate bandwidth as configured.
  - FRR protection type (whether or not to provide bandwidth protection for the primary CRLSP) changes.

Procedures

1. Configure IP addresses for interfaces:

Configure IP addresses and masks for interfaces on Switch A, including the loopback interface, as shown in Figure 3.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port twenty-fivegige 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 2.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
```

```
[SwitchA-LoopBack0] quit
```

Configure other devices in the same way that Switch A is configured. (Details not shown.)

2. Configure OSPF to ensure IP connectivity among the switches:

Configure Switch A.

```
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure Switch B.

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 2.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure Switch C.

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 3.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Configure Switch D.

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SwitchD-ospf-1-area-0.0.0.0] network 4.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Configure Switch E.

```
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[SwitchE-ospf-1-area-0.0.0.0] network 3.2.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 3.3.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

Execute the **display ip routing-table** command on each switch to verify that the switches have learned the routes to one another, including the routes to the loopback interfaces. The following shows the output on Switch A.

```
[SwitchA] display ip routing-table
```

```
Destinations : 19        Routes : 19

Destination/Mask    Proto   Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct  0    0           127.0.0.1       InLoop0
1.1.1.1/32          Direct  0    0           127.0.0.1       InLoop0
2.1.1.0/24          Direct  0    0           2.1.1.1         Vlan2
2.1.1.0/32          Direct  0    0           2.1.1.1         Vlan2
2.1.1.1/32          Direct  0    0           127.0.0.1       InLoop0
2.1.1.255/32        Direct  0    0           2.1.1.1         Vlan2
2.2.2.2/32          O_INTRA 10   1           2.1.1.2         Vlan2
3.1.1.0/24          O_INTRA 10   2           2.1.1.2         Vlan2
3.2.1.0/24          O_INTRA 10   2           2.1.1.2         Vlan2
3.3.1.0/24          O_INTRA 10   3           2.1.1.2         Vlan2
3.3.3.3/32          O_INTRA 10   2           2.1.1.2         Vlan2
4.1.1.0/24          O_INTRA 10   3           2.1.1.2         Vlan2
4.4.4.4/32          O_INTRA 10   3           2.1.1.2         Vlan2
5.5.5.5/32          O_INTRA 10   2           2.1.1.2         Vlan2
127.0.0.0/8         Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
255.255.255.255/32  Direct  0    0           127.0.0.1       InLoop0
```

3. Configure an LSR ID, and enable MPLS, MPLS TE, and RSVP-TE on each switch. Enable BFD for RSVP-TE on Switch B and Switch C:

Configure Switch A.

```
[SwitchA] mpls lsr-id 1.1.1.1
[SwitchA] mpls te
[SwitchA-te] quit
[SwitchA] rsvp
[SwitchA-rsvp] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] mpls enable
[SwitchA-Vlan-interface2] mpls te enable
[SwitchA-Vlan-interface2] rsvp enable
[SwitchA-Vlan-interface2] quit
```

Configure Switch B.

```
[SwitchB] mpls lsr-id 2.2.2.2
[SwitchB] mpls te
[SwitchB-te] quit
[SwitchB] rsvp
[SwitchB-rsvp] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls enable
[SwitchB-Vlan-interface2] mpls te enable
[SwitchB-Vlan-interface2] rsvp enable
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] mpls enable
```

```
[SwitchB-Vlan-interface3] mpls te enable
[SwitchB-Vlan-interface3] rsvp enable
[SwitchB-Vlan-interface3] rsvp bfd enable
[SwitchB-Vlan-interface3] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] mpls enable
[SwitchB-Vlan-interface5] mpls te enable
[SwitchB-Vlan-interface5] rsvp enable
[SwitchB-Vlan-interface5] quit
```

Configure Switch C.

```
[SwitchC] mpls lsr-id 3.3.3.3
[SwitchC] mpls te
[SwitchC-te] quit
[SwitchC] rsvp
[SwitchC-rsvp] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] mpls enable
[SwitchC-Vlan-interface3] mpls te enable
[SwitchC-Vlan-interface3] rsvp enable
[SwitchC-Vlan-interface3] rsvp bfd enable
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] mpls enable
[SwitchC-Vlan-interface4] mpls te enable
[SwitchC-Vlan-interface4] rsvp enable
[SwitchC-Vlan-interface4] quit
[SwitchC] interface vlan-interface 6
[SwitchC-Vlan-interface6] mpls enable
[SwitchC-Vlan-interface6] mpls te enable
[SwitchC-Vlan-interface6] rsvp enable
[SwitchC-Vlan-interface6] quit
```

Configure Switch D.

```
[SwitchD] mpls lsr-id 4.4.4.4
[SwitchD] mpls te
[SwitchD-te] quit
[SwitchD] rsvp
[SwitchD-rsvp] quit
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] mpls enable
[SwitchD-Vlan-interface4] mpls te enable
[SwitchD-Vlan-interface4] rsvp enable
[SwitchD-Vlan-interface4] quit
```

Configure Switch E.

```
[SwitchE] mpls lsr-id 5.5.5.5
[SwitchE] mpls te
[SwitchE-te] quit
[SwitchE] rsvp
[SwitchE-rsvp] quit
```

```
[SwitchE] interface vlan-interface 5
[SwitchE-Vlan-interface5] mpls enable
[SwitchE-Vlan-interface5] mpls te enable
[SwitchE-Vlan-interface5] rsvp enable
[SwitchE-Vlan-interface5] quit
[SwitchE] interface vlan-interface 6
[SwitchE-Vlan-interface6] mpls enable
[SwitchE-Vlan-interface6] mpls te enable
[SwitchE-Vlan-interface6] rsvp enable
[SwitchE-Vlan-interface6] quit
```

4. Configure MPLS TE attributes of links:

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch A.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] mpls te max-link-bandwidth 50000
[SwitchA-Vlan-interface2] mpls te max-reservable-bandwidth 40000
[SwitchA-Vlan-interface2] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch B.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls te max-link-bandwidth 50000
[SwitchB-Vlan-interface2] mpls te max-reservable-bandwidth 40000
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] mpls te max-link-bandwidth 50000
[SwitchB-Vlan-interface3] mpls te max-reservable-bandwidth 40000
[SwitchB-Vlan-interface3] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] mpls te max-link-bandwidth 50000
[SwitchB-Vlan-interface5] mpls te max-reservable-bandwidth 40000
[SwitchB-Vlan-interface5] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch C.

```
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] mpls te max-link-bandwidth 50000
[SwitchC-Vlan-interface3] mpls te max-reservable-bandwidth 40000
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] mpls te max-link-bandwidth 50000
[SwitchC-Vlan-interface4] mpls te max-reservable-bandwidth 40000
[SwitchC-Vlan-interface4] quit
[SwitchC] interface vlan-interface 6
[SwitchC-Vlan-interface6] mpls te max-link-bandwidth 50000
[SwitchC-Vlan-interface6] mpls te max-reservable-bandwidth 40000
[SwitchC-Vlan-interface6] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch D.

```
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] mpls te max-link-bandwidth 50000
[SwitchD-Vlan-interface4] mpls te max-reservable-bandwidth 40000
[SwitchD-Vlan-interface4] quit
```

Configure the maximum link bandwidth and maximum reservable bandwidth on Switch E.

```
[SwitchE] interface vlan-interface 5
[SwitchE-Vlan-interface5] mpls te max-link-bandwidth 50000
[SwitchE-Vlan-interface5] mpls te max-reservable-bandwidth 40000
[SwitchE-Vlan-interface5] quit
[SwitchE] interface vlan-interface 6
[SwitchE-Vlan-interface6] mpls te max-link-bandwidth 50000
[SwitchE-Vlan-interface6] mpls te max-reservable-bandwidth 40000
[SwitchE-Vlan-interface6] quit
```

5. Configure OSPF TE to advertise link TE attributes:

Enable opaque LSA advertisement and reception on Switch A. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchA] ospf
[SwitchA-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch A.

```
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] mpls te enable
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch B. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchB] ospf
[SwitchB-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch B.

```
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] mpls te enable
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch C. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchC] ospf
[SwitchC-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch C.

```
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] mpls te enable
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch D. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchD] ospf
[SwitchD-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch D.

```
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] mpls te enable
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

Enable opaque LSA advertisement and reception on Switch E. By default, the opaque LSA advertisement and reception capability is enabled.

```
[SwitchE] ospf
```

```
[SwitchE-ospf-1] opaque-capability enable
```

Enable MPLS TE for OSPF area 0 on Switch E.

```
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] mpls te enable
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

6. Configure an MPLS TE tunnel on Switch A (the ingress node of the primary CRLSP):

Configure an explicit path named **pri-path** for the primary CRLSP.

```
[SwitchA] explicit-path pri-path
[SwitchA-explicit-path-pri-path] nexthop 2.1.1.2
[SwitchA-explicit-path-pri-path] nexthop 3.1.1.3
[SwitchA-explicit-path-pri-path] nexthop 4.1.1.4
[SwitchA-explicit-path-pri-path] nexthop 4.4.4.4
[SwitchA-explicit-path-pri-path] quit
```

Configure MPLS TE tunnel interface Tunnel 4 for the primary CRLSP.

```
[SwitchA] interface tunnel4 mode mpls-te
[SwitchA-Tunnel4] ip address 10.1.1.1 255.255.255.0
```

Specify the tunnel destination address as the LSR ID of Switch D, configure MPLS TE to use RSVP-TE to establish the tunnel, and assign 30000 kbps bandwidth to the tunnel.

```
[SwitchA-Tunnel4] destination 4.4.4.4
[SwitchA-Tunnel4] mpls te signaling rsvp-te
[SwitchA-Tunnel4] mpls te bandwidth 30000
```

Specify the explicit path to be used as **pri-path**.

```
[SwitchA-Tunnel4] mpls te path preference 1 explicit-path pri-path
```

Enable FRR for the MPLS TE tunnel.

```
[SwitchA-Tunnel4] mpls te fast-reroute
[SwitchA-Tunnel4] quit
```

Execute the **display interface tunnel brief** command on Switch A. The output shows that tunnel interface Tunnel 4 is up.

```
[SwitchA] display interface tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun4                 UP   UP       10.1.1.1
```

Execute the **display mpls te tunnel-interface** command on Switch A to display detailed information about the MPLS TE tunnel.

```
[SwitchA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 37325           Tunnel ID            : 4
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
```

```
  Reverse-LSP LSR ID   : -              Reverse-LSP Tunnel ID: -
  Class Type           : CT0            Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7              Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled        Record Label         : Enabled
  FRR Flag             : Enabled        Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled       Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No             Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3              Retry Interval       : 2 sec
  Reoptimization       : Disabled       Reoptimization Freq  : -
  Backup Type          : None           Backup LSP ID        : -
  Auto Bandwidth       : Disabled       Auto Bandwidth Freq  : -
  Min Bandwidth        : -              Max Bandwidth        : -
  Collected Bandwidth  : -
```

7. Configure a bypass tunnel on Switch B (the PLR):

Configure an explicit path named **by-path** for the bypass tunnel.

```
[SwitchB] explicit-path by-path
[SwitchB-explicit-path-by-path] nexthop 3.2.1.5
[SwitchB-explicit-path-by-path] nexthop 3.3.1.3
[SwitchB-explicit-path-by-path] nexthop 3.3.3.3
[SwitchB-explicit-path-by-path] quit
```

Configure MPLS TE tunnel interface Tunnel 5 for the bypass tunnel.

```
[SwitchB] interface tunnel 5 mode mpls-te
[SwitchB-Tunnel5] ip address 11.1.1.1 255.255.255.0
```

Specify the tunnel destination address as the LSR ID of Switch C and configure MPLS TE to use RSVP-TE to establish the tunnel.

```
[SwitchB-Tunnel5] destination 3.3.3.3
[SwitchB-Tunnel5] mpls te signaling rsvp-te
```

Set the bandwidth that the bypass tunnel can protect to 30000 kbps.

```
[SwitchB-Tunnel5] mpls te backup bandwidth 30000
```

Specify the explicit path to be used as **by-path**.

```
[SwitchB-Tunnel5] mpls te path preference 1 explicit-path by-path
[SwitchB-Tunnel5] quit
```

Bind the bypass tunnel to the protected interface.

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] mpls te fast-reroute bypass-tunnel tunnel 5
[SwitchB-Vlan-interface3] quit
```

Execute the **`display interface tunnel brief`** command on Switch B. The output shows that tunnel interface Tunnel 5 is up.

```
[SwitchB] display interface tunnel brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
```

```
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun5                 UP   DOWN     11.1.1.1
```

8. Configure a static route on Switch A to direct traffic destined for 4.1.1.0/24 to MPLS TE tunnel interface Tunnel 4.

```
[SwitchA] ip route-static 4.1.1.0 24 tunnel 4 preference 1
```

Verifying the configuration

Execute the **display mpls lsp** command on each switch. The output shows the LSP entries. Switch B has two CRLSPs. The bypass tunnel backs up the primary CRLSP.

```
[SwitchA] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325            RSVP     -/1150          Vlan2
2.1.1.2                    Local    -/-             Vlan2
Tunnel4                    Local    -/-             NHLFE1026
[SwitchB] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325            RSVP     1150/1147       Vlan3
Backup                              1150/1147       Tun5
2.2.2.2/5/18928            RSVP     -/1149          Vlan5
3.1.1.3                    Local    -/-             Vlan3
3.2.1.5                    Local    -/-             Vlan5
Tunnel5                    Local    -/-             NHLFE1027
[SwitchC] display mpls lsp
FEC                        Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325            RSVP     1147/3          Vlan4
2.2.2.2/5/18928            RSVP     3/-             -
4.1.1.4                    Local    -/-             Vlan4
```

Shut down the protected interface VLAN-interface 3 on the PLR (Switch B).

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] shutdown
[SwitchB-Vlan-interface3] quit
```

Execute the **display interface tunnel 4 brief** command on Switch A to display information about the primary CRLSP. The output shows that the tunnel interface is still up.

```
[SwitchA] display interface tunnel 4 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
Tun4                 UP   UP       10.1.1.1
```

Execute the **display mpls te tunnel-interface** command on Switch A to display detailed information about the tunnel interface.

```
[SwitchA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 4
Tunnel State           : Up (Main CRLSP up, Shared-resource CRLSP being set up)
Tunnel Attributes      :
  LSP ID               : 37325           Tunnel ID            : 4
```

```
  Admin State          : Normal
  Ingress LSR ID       : 1.1.1.1         Egress LSR ID        : 4.4.4.4
  Signaling            : RSVP-TE         Static CRLSP Name    : -
  Resv Style           : SE
  Tunnel mode          : -
  Reverse-LSP name     : -
  Reverse-LSP LSR ID   : -               Reverse-LSP Tunnel ID: -
  Class Type           : CT0             Tunnel Bandwidth     : 30000 kbps
  Reserved Bandwidth   : 30000 kbps
  Setup Priority       : 7               Holding Priority     : 7
  Affinity Attr/Mask   : 0/0
  Explicit Path        : pri-path
  Backup Explicit Path : -
  Metric Type          : TE
  Record Route         : Enabled         Record Label         : Enabled
  FRR Flag             : Enabled         Bandwidth Protection : Disabled
  Backup Bandwidth Flag: Disabled        Backup Bandwidth Type: -
  Backup Bandwidth     : -
  Bypass Tunnel        : No              Auto Created         : No
  Route Pinning        : Disabled
  Retry Limit          : 3               Retry Interval       : 2 sec
  Reoptimization       : Disabled        Reoptimization Freq  : -
  Backup Type          : None            Backup LSP ID        : -
  Auto Bandwidth       : Disabled        Auto Bandwidth Freq  : -
  Min Bandwidth        : -               Max Bandwidth        : -
  Collected Bandwidth  : -
```

Execute the **display mpls lsp** command on Switch B. The output shows that the bypass tunnel is in use.

```
[SwitchB] display mpls lsp
FEC                       Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/4/37325           RSVP     1150/1147       Tun5
2.2.2.2/5/18928           RSVP     -/1149          Vlan5
3.2.1.5                   Local    -/-             Vlan5
Tunnel5                   Local    -/-             NHLFE1027
```

On the PLR, configure the interval for selecting an optimal bypass tunnel as 5 seconds.

```
[SwitchB] mpls te
[SwitchB-te] fast-reroute timer 5
[SwitchB-te] quit
```

On the PLR, bring up the protected interface VLAN-interface 3.

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] undo shutdown
[SwitchB-Vlan-interface3] quit
```

Execute the **display interface tunnel 4 brief** command on Switch A. The output shows that the tunnel interface is in up state.

```
[SwitchA] display interface tunnel 4 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

```
Interface            Link Protocol Primary IP      Description
Tun4                 UP   UP       10.1.1.1
```

Wait for about 5 seconds, execute the **display mpls lsp verbose** command on Switch B. The output shows that Tunnel 5 is bound to interface VLAN-interface 3 but is not in use.

```
[SwitchB] display mpls lsp verbose
Destination  : 4.4.4.4
FEC          : 1.1.1.1/4/53319
Protocol     : RSVP
LSR Type     : Transit
Service      : -
In-Label     : 1150
Path ID      : 0x540000003.1
State        : Active
Out-Label    : 1150
Nexthop      : 3.1.1.3
Out-Interface: Vlan3
BkLabel      : 1150
BkInterface  : Tun5

Destination  : 3.3.3.3
FEC          : 2.2.2.2/5/16429
Protocol     : RSVP
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1025
State        : Active
Out-Label    : 1151
Nexthop      : 3.2.1.5
Out-Interface: Vlan5

Destination  : 3.1.1.3
FEC          : 3.1.1.3
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1027
State        : Active
Nexthop      : 3.1.1.3
Out-Interface: Vlan3

Destination  : 3.2.1.5
FEC          : 3.2.1.5
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 1024
State        : Active
Nexthop      : 3.2.1.5
```

```
Out-Interface: Vlan5

Destination  : 3.3.3.3
FEC          : Tunnel5
Protocol     : Local
LSR Type     : Ingress
Service      : -
NHLFE ID     : 268435461
State        : Active
Out-Interface: NHLFE1025
```

Execute the **`display ip routing-table`** command on Switch A. The output shows a static route entry with interface Tunnel 4 as the output interface.

```
[SwitchA] display ip routing-table

Destinations : 23        Routes : 23

Destination/Mask    Proto   Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct  0    0            127.0.0.1       InLoop0
1.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
2.1.1.0/24          Direct  0    0            2.1.1.1         Vlan2
2.1.1.0/32          Direct  0    0            2.1.1.1         Vlan2
2.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
2.1.1.255/32        Direct  0    0            2.1.1.1         Vlan2
2.2.2.2/32          O_INTRA 10   1            2.1.1.2         Vlan2
3.1.1.0/24          O_INTRA 10   2            2.1.1.2         Vlan2
3.2.1.0/24          O_INTRA 10   2            2.1.1.2         Vlan2
3.3.1.0/24          O_INTRA 10   3            2.1.1.2         Vlan2
3.3.3.3/32          O_INTRA 10   2            2.1.1.2         Vlan2
4.1.1.0/24          Static  1    0            0.0.0.0         Tun4
4.4.4.4/32          O_INTRA 10   3            2.1.1.2         Vlan2
5.5.5.5/32          O_INTRA 10   2            2.1.1.2         Vlan2
10.1.1.0/24         Direct  0    0            10.1.1.1        Tun4
10.1.1.0/32         Direct  0    0            10.1.1.1        Tun4
10.1.1.1/32         Direct  0    0            127.0.0.1       InLoop0
10.1.1.255/32       Direct  0    0            10.1.1.1        Tun4
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
255.255.255.255/32  Direct  0    0            127.0.0.1       InLoop0
```

Configuration files

- Switch A:

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
```

```
  network 2.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 1.1.1.1
#
vlan 2
#
mpls te
#
explicit-path pri-path
 nexthop index 1 2.1.1.2 include strict
 nexthop index 101 3.1.1.3 include strict
 nexthop index 201 4.1.1.4 include strict
 nexthop index 301 4.4.4.4 include strict
#
rsvp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface2
 ip address 2.1.1.1 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 2
#
interface Tunnel4 mode mpls-te
 ip address 10.1.1.1 255.255.255.0
 mpls te bandwidth ct0 30000
 mpls te path preference 1 explicit-path pri-path
 mpls te fast-reroute
 destination 4.4.4.4
#
ip route-static 4.1.1.0 24 Tunnel4 preference 1
#
```

- Switch B:

```
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  network 3.1.1.0 0.0.0.255
```

```
  network 3.2.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 2.2.2.2
#
vlan 2 to 3
#
vlan 5
#
mpls te
  fast-reroute timer 5
#
explicit-path by-path
 nexthop index 1 3.2.1.5 include strict
 nexthop index 101 3.3.1.3 include strict
 nexthop index 201 3.3.3.3 include strict
#
rsvp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface2
 ip address 2.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface3
 ip address 3.1.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 mpls te fast-reroute bypass-tunnel Tunnel5
 rsvp enable
 rsvp bfd enable
#
interface Vlan-interface5
 ip address 3.2.1.2 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
```

```
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 2
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 3
#
interface Twenty-FiveGigE1/0/3
 port link-mode bridge
 port access vlan 5
#
interface Tunnel5 mode mpls-te
 ip address 11.1.1.1 255.255.255.0
 mpls te backup bandwidth ct0 30000
 mpls te path preference 1 explicit-path by-path
 destination 3.3.3.3
#
```

- Switch C:

```
#
ospf 1
 area 0.0.0.0
  network 3.1.1.0 0.0.0.255
  network 3.3.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  network 4.1.1.0 0.0.0.255
  mpls te enable
#
 mpls lsr-id 3.3.3.3
#
vlan 3 to 4
#
vlan 6
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface3
 ip address 3.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
```

```
 rsvp bfd enable
#
interface Vlan-interface4
 ip address 4.1.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface6
 ip address 3.3.1.3 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 4
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 3
#
interface Twenty-FiveGigE1/0/3
 port link-mode bridge
 port access vlan 6
#
```

- Switch D:

```
#
ospf 1
 area 0.0.0.0
  network 4.1.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
  mpls te enable
#
 mpls lsr-id 4.4.4.4
#
vlan 4
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
```

```
#
interface Vlan-interface4
 ip address 4.1.1.4 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 4
#
```

- Switch E:

```
#
ospf 1
 area 0.0.0.0
  network 3.2.1.0 0.0.0.255
  network 3.3.1.0 0.0.0.255
  network 5.5.5.5 0.0.0.0
  mpls te enable
#
 mpls lsr-id 5.5.5.5
#
vlan 5 to 6
#
mpls te
#
rsvp
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
interface Vlan-interface5
 ip address 3.2.1.5 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
#
interface Vlan-interface6
 ip address 3.3.1.5 255.255.255.0
 mpls enable
 mpls te enable
 mpls te max-link-bandwidth 50000
 mpls te max-reservable-bandwidth 40000
 rsvp enable
```

```
#
interface Twenty-FiveGigE1/0/1
 port link-mode bridge
 port access vlan 5
#
interface Twenty-FiveGigE1/0/2
 port link-mode bridge
 port access vlan 6
#
```

Contents

Introduction

This chapter provides examples for configuring control plane-based QoS policies.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of QoS policies.

Example: Rate limiting ICMP packets

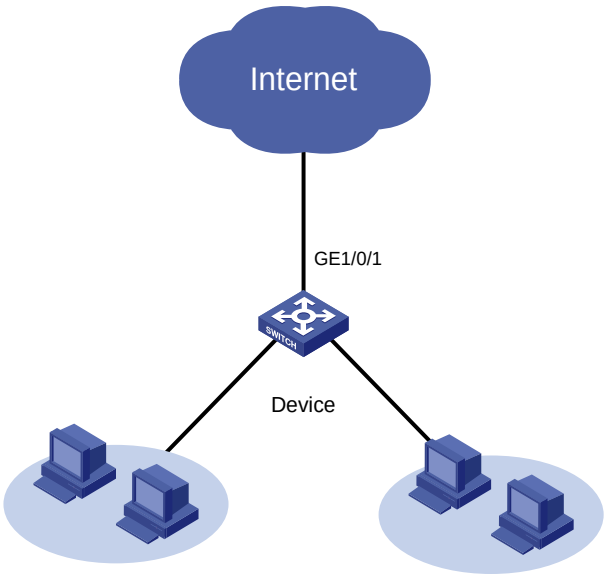
Network configuration

As shown in Figure 1, the device receives a large number of ICMP packets from the Internet. As a result, CPU usage is high, and device performance degrades.

Configure a control plane-based QoS policy to meet the following requirements:

- Rate limit ICMP packets sent to the control plane to 320 kbps.
- Drop excess ICMP packets.

Figure 1 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Use the **`if-match`** command to classify ICMP packets into a class.
- Use the **`car`** command to configure the rate limit value for ICMP packets and drop excess packets.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	不Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 63xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series	Release 11xx

Hardware	Software version
S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 63xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 11xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 63xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 11xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

When you configure a control plane-based QoS policy to rate limit ICMP packets, follow these restrictions and guidelines:

- By default, the predefined QoS policy is applied to the control plane. The predefined QoS policy identifies packet types by system index and uses a default rate limit value for each packet type. To display the predefined QoS policy, use the **`display qos policy control-plane pre-defined`** command.
- You can use the **`if-match control-plane protocol`** or **`if-match control-plane protocol-group`** command to classify protocol packets.
- You can only configure the **`car`** command or a combination of the **`car`** and **`accounting packet`** commands in the behavior associated with the class.

Procedures

Create a class named **ICMP**, and use the ICMP protocol as the match criterion.

```
<Device> system-view
[Device] traffic classifier ICMP
[Device-classifier-ICMP] if-match control-plane protocol icmp
[Device-classifier-ICMP] quit
```

Create a behavior named **ICMP**, and configure a CAR action for ICMP packets.

```
[Device] traffic behavior ICMP
[Device-behavior-ICMP] car cir 320
[Device-behavior-ICMP] quit
```

Create a QoS policy named **ICMP**, and associate the class **ICMP** with the behavior **ICMP** in the QoS policy.

```
[Device] qos policy ICMP
[Device-qospolicy-ICMP] classifier ICMP behavior ICMP
[Device-qospolicy-ICMP] quit
```

Apply the QoS policy **ICMP** to the inbound direction of the control plane.

```
[Device] control-plane slot 1
[Device-cp-slot1] qos apply policy ICMP inbound
[Device-cp-slot1] quit
```

Verifying the configuration

Verify that the QoS policy is correctly applied to the control plane.

```
[Device] display qos policy control-plane slot 1
Control plane slot 1
  Direction: Inbound
  Policy: ICMP
   Classifier: ICMP
     Operator: AND
     Rule(s) :
      If-match control-plane protocol icmp
     Behavior: ICMP
      Committed Access Rate:
```

```
        CIR 320 (kbps), CBS 20480 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
```

Configuration files

```
#
traffic classifier ICMP operator and
 if-match control-plane protocol icmp
#
traffic behavior ICMP
 car cir 320 cbs 20480 ebs 0 green pass red discard yellow pass
#
qos policy ICMP
 classifier ICMP behavior ICMP
#
control-plane slot 1
 qos apply policy ICMP inbound
```

Contents

Introduction

This document provides examples for configuring priority mapping and queue scheduling profiles.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of priority mapping and queue scheduling profiles.

Example: Configuring priority mapping and queue scheduling

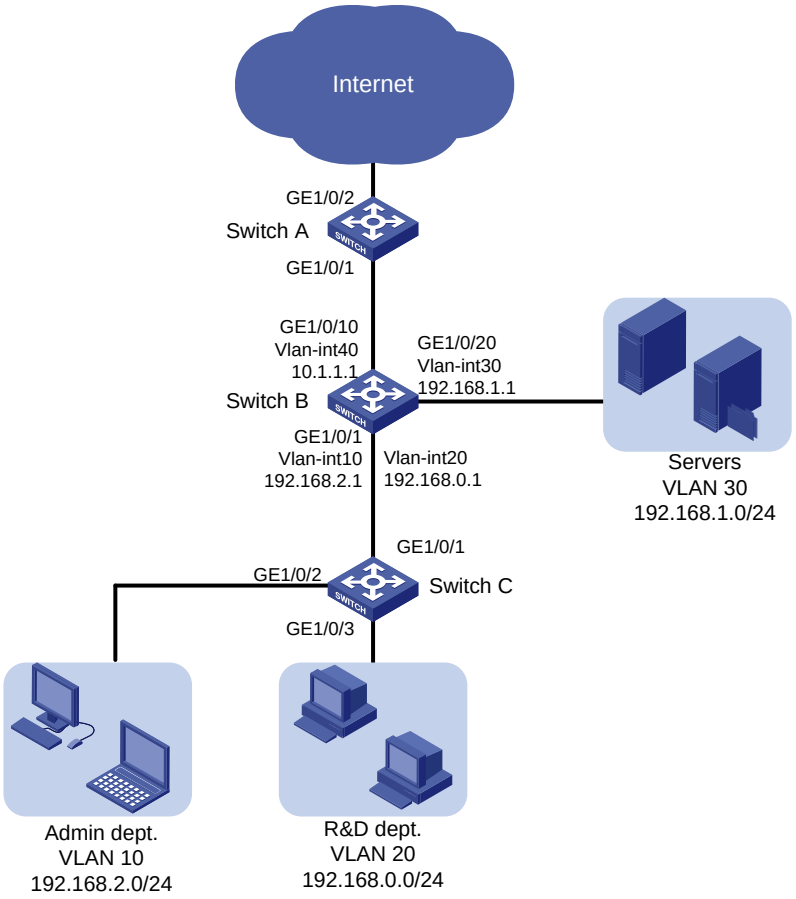
Network configuration

As shown in Figure 1, the Internet-accessing traffic includes the following types: HTTP, FTP, and Email, with the DSCP values 33, 35, and 27, respectively.

Configure priority mapping and queue scheduling to meet the following requirements:

- **Access to the internal server farm**—The traffic from the Administration department takes priority over the traffic from the R&D department. When congestion occurs, they are scheduled at a ratio of 2:1.
- **Access to the Internet**—The traffic from the Administration department takes priority over the traffic from the R&D department. When congestion occurs, the traffic from the Administration department is scheduled preferentially. The traffic from the R&D department is scheduled when no traffic from the Administration department exists. The three types of Internet-accessing traffic are transmitted in the following priority order: HTTP > FTP > Email. When congestion occurs, the three types of traffic are transmitted at a ratio of 2:1:1.

Figure 1 Network diagram



Analysis

Priority configuration for the internal network traffic

To meet the network requirements, you must perform the following tasks:

- For packets from the two departments to be marked with different 802.1p priorities, configure different port priority values for the interfaces connected to the two departments.
- Because the 802.1p priorities are carried in VLAN tags, you must configure GigabitEthernet 1/0/1 on Switch C to send packets carrying VLAN tags. This example uses the port link type **trunk**.
- To make the marked 802.1p priority actually affect the packet transmission, configure trusting the 802.1p priorities of received packets on all input interfaces along the transmission path.
- To schedule packets from different queues at the specified ratio when congestion occurs, enable WRR queuing and configure different weights for queues.

Priority configuration for the Internet traffic

To meet the network requirements, you must perform the following tasks:

- To completely prioritize the traffic from the Administration department when the interface is congested in the outbound direction, perform the following tasks:
  - Configure SP queuing on the interface.

    - Assign the traffic from the Administration department to a higher-priority queue.
- To determine the transmission priority based on the upper-layer protocols, configure trusting the DSCP values on the interface, so that the interface can enqueue packets based on the DSCP values.
- To assign packets with DSCP value 33 to a higher-priority queue, modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to a higher 802.1p priority value than the default. By default, DSCP values 33, 35, 27 are mapped to local precedence values 4, 4, and 3, respectively, based on the DSCP-to-802.1p priority mapping table and the 802.1p-to-local priority mapping table.
- To schedule packets from different queues at the specified ratio when congestion occurs, enable WRR queuing and configure different weights for queues.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx

Hardware	Software version
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Procedures

Configuring transmission priorities for the internal network traffic

1. Configure Switch C:

Create VLANs 10 and 20.

```
<SwitchC> system-view
[SwitchC] vlan 10
[SwitchC-vlan10] quit
[SwitchC] vlan 20
[SwitchC-vlan20] quit
```

Assign interface GigabitEthernet 1/0/2 to VLAN 10, and set the port priority to 6 for the interface. This enables the traffic from the Administration department to be marked with 802.1p priority value 6.

```
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 10
[SwitchC-GigabitEthernet1/0/2] qos priority 6
[SwitchC-GigabitEthernet1/0/2] quit
```

Assign interface GigabitEthernet 1/0/3 to VLAN 20, and set the port priority to 4 for the interface. This enables the traffic from the R&D department to be marked with 802.1p priority value 4.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port access vlan 20
[SwitchC-GigabitEthernet1/0/3] qos priority 4
[SwitchC-GigabitEthernet1/0/3] quit
```

Configure interface GigabitEthernet 1/0/1 as a trunk port, assign the interface to VLAN 10 and VLAN 20, and remove the interface from VLAN 1.

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[SwitchC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[SwitchC-GigabitEthernet1/0/1] quit
```

2. Configure Switch B:

Create VLANs 10, 20, 30, and 40.

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] vlan 20
[SwitchB-vlan20] quit
[SwitchB] vlan 30
[SwitchB-vlan30] quit
[SwitchB] vlan 40
[SwitchB-vlan40] quit
```

Configure interface GigabitEthernet 1/0/1 as a trunk port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

Assign interface GigabitEthernet 1/0/1 to VLANs 10 and 20.

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
```

Remove interface GigabitEthernet 1/0/1 from VLAN 1.

```
[SwitchB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

Configure GigabitEthernet 1/0/1 to trust the 802.1p priority of received packets. Based on the 802.1p-to-local priority mapping table, traffic with 802.1p priority 4 is assigned to queue 4, and traffic with 802.1p priority 6 is assigned to queue 6.

```
[SwitchB-GigabitEthernet1/0/1] qos trust dot1p
[SwitchB-GigabitEthernet1/0/1] quit
```

Assign interface GigabitEthernet 1/0/20 to VLAN 30.

```
[SwitchB] interface gigabitethernet 1/0/20
[SwitchB-GigabitEthernet1/0/20] port access vlan 30
```

Create VLAN interfaces and configure routing protocols to enable communication between network segments. For more information about these configurations, see *Layer 3—IP Routing Configuration Guide* in the configuration guides for you switch.

Enable packet-count WRR on interface GigabitEthernet 1/0/20. By default, byte-count WRR is enabled.

```
[SwitchB-GigabitEthernet1/0/20] qos wrr weight
```

Configure the weight of queue 6 as two times that of queue 4. In this example, set the weight value to 4 for queue 6 and 2 for queue 4.

```
[SwitchB-GigabitEthernet1/0/20] qos wrr 4 group 1 weight 2
[SwitchB-GigabitEthernet1/0/20] qos wrr 6 group 1 weight 4
[SwitchB-GigabitEthernet1/0/20] quit
```

Assign interface GigabitEthernet 1/0/10 to VLAN 40.

```
[SwitchB] interface gigabitethernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port access vlan 40
[SwitchB-GigabitEthernet1/0/10] quit
```

Configuring transmission priorities for the traffic to the Internet

1. Configure Switch B:

Enable SP queuing on interface GigabitEthernet 1/0/10.

```
[SwitchB] interface gigabitethernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] qos sp
```

2. Configure Switch A:

   # Configure interface GigabitEthernet 1/0/1 to trust the DSCP values of received packets.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] qos trust dscp
```

   # Modify the DSCP-to-802.1p priority mapping table to map DSCP value 33 to 802.1p priority 5 (queue 5).

```
[SwitchA] qos map-table dscp-dot1p
[SwitchA-maptbl-dscp-dot1p] import 33 export 5
[SwitchA-maptbl-dscp-dot1p] quit
```

   The configuration assigns the three types of packets (HTTP, FTP, and Email) to queues 5, 4, and 3, respectively.

   # Enable packet-count WRR on interface GigabitEthernet 1/0/2. By default, byte-count WRR is enabled.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] qos wrr weight
```

   # Set the weights of the three queues at a ratio of 2:1:1 (6, 3, and 3 in this example).

```
[SwitchA-GigabitEthernet1/0/2] qos wrr 5 group 1 weight 6
[SwitchA-GigabitEthernet1/0/2] qos wrr 4 group 1 weight 3
[SwitchA-GigabitEthernet1/0/2] qos wrr 3 group 1 weight 3
```

Verifying the configuration

Verify the configuration on any interface on any switch, for example, GigabitEthernet 1/0/2 on Switch A.

Verify the WRR configuration.

```
[SwitchA] display qos queue wrr interface gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/2
Queue ID     Queue name     Group     Weight
 ------------------------------------------------------
 0            be             1         1
 1            af1            1         2
 2            af2            1         3
 3            af3            1         3
 4            af4            1         3
 5            ef             1         6
 6            cs6            1         13
 7            cs7            1         15
```

Configuration files

IMPORTANT:

The **`port link-mode bridge`** command might be displayed in the configuration files of some switches.

- Switch A:

```
#
qos map-table dscp-dot1p
 import 33 export 5
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos trust dscp
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos wrr af3 group 1 weight 3
 qos wrr af4 group 1 weight 3
 qos wrr ef group 1 weight 6
#
return
```

- Switch B:

```
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 qos trust dot1p
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 40
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 port access vlan 30
 qos wrr af4 group 1 weight 2
 qos wrr cs6 group 1 weight 4
#
return
```

- Switch C:

```
#
vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 qos priority 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 20
 qos priority 4
#
return
```

Contents

Introduction

This document provides configuration examples of ARP attack protection.

ARP is easy to use but it does not have any security mechanisms. Attackers can easily attack the network by sending forged ARP packets. The device provides various ARP attack protection measures to prevent, detect, and resolve ARP attacks and ARP viruses on LANs.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of ARP attack protection.

Example: Configuring ARP attack protection

Network configuration

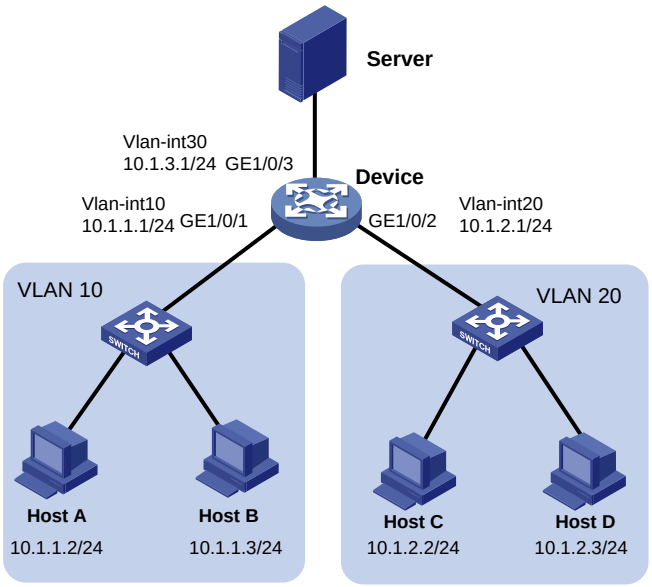
As shown in Figure 1, the device connects to the server through GE1/0/3 as a gateway and connects to Host A and Host B in VLAN 10, and Host C and Host D in VLAN 20 through GE1/0/1 and GE1/0/2, respectively.

Configure ARP attack protection on the device to prevent the following ARP threats:

- Host A sends forged ARP packets and forged gratuitous ARP packets to the device to edit the ARP entries on the device maliciously. As a result, other users cannot receive data packets normally.
- Host C sends a large number of unresolvable IP packets to attack the device, causing the following results:
  - The device CPU is busy, affecting normal service processing.
  - The device sends a large number of ARP requests, overloading the target subnets.
- Host D launches ARP flood attacks by sending a large number of ARP packets with different source IP addresses but fixed MAC address. Such attacks run out the ARP table resources on the device and cause a busy CPU, affecting normal service processing.

Besides, Host B might send a large number of ARP packets to the device. This is normal ARP behavior required by services. Do not filter out packets sent from Host B when you configure ARP attack protection.

Figure 1 Network diagram



Analysis

To meet the network requirements, configure the device as follows:

- To prevent forged ARP packets sent by Host A from updating the ARP entries on the device, configure ARP blackhole routing and ARP active acknowledgement in strict mode.
- To prevent the forged gratuitous ARP packets sent by Host A from updating the ARP entries on the device, disable gratuitous ARP packet learning.
- To avoid unresolvable packets sent by Host C, enable ARP source suppression and set the maximum number of unresolvable packets that the device can process per source IP address within 5 seconds.
- To avoid ARP flood attacks caused by ARP packets with the same IP address, enable ARP packet rate limit and set the limit rate. When Host C launches ARP flood attacks on the device by sending a large number of ARP packets with the same source IP address, the device discards the packets that exceed the limit rate to avoid a busy CPU.
- To avoid ARP flood attacks caused by ARP packets with different IP addresses but fixed MAC address sent by Host D, configure source MAC-based ARP attack detection. If you fail to configure this feature, the ARP table resources run out and the CPU is busy. To avoid filtering out packets sent by Host B, exclude the MAC address of Host B from this detection.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx

Hardware	Software version
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx

Hardware	Software version
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6658P01 and later

Restrictions and guidelines

When you configure ARP attack protection, follow these restrictions and guidelines:

- When you configure ARP active acknowledgement in strict mode, make sure ARP blackhole routing is enabled.
- After you disable gratuitous ARP packet learning, the device does not create ARP entries when receiving gratuitous ARP packets, but updates the existing corresponding ARP entries. If you

do not want the device to create ARP entries for gratuitous ARP packets, disable gratuitous ARP packet learning to save ARP entry resources.

Procedures

Configuring VLANs and interface IP addresses

(Optional.) Configure the operating mode of GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as Layer 2.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-mode bridge
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] port link-mode bridge
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] port link-mode bridge
[Device-GigabitEthernet1/0/3] quit
```

Create VLAN 10, and assign GigabitEthernet 1/0/1 to the VLAN.

```
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
```

Create VLAN-interface 10, and assign IP address 10.1.1.1/24 to it.

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
[Device-Vlan-interface10] quit
```

Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.

```
[Device] vlan 20
[Device-vlan20] port gigabitethernet 1/0/2
[Device-vlan20] quit
```

Create VLAN-interface 20, and assign IP address 10.1.2.1/24 to it.

```
[Device] interface vlan-interface 20
[Device-Vlan-interface20] ip address 10.1.2.1 255.255.255.0
[Device-Vlan-interface20] quit
```

Create VLAN 30, and assign GigabitEthernet 1/0/3 to the VLAN.

```
[Device] vlan 30
[Device-vlan30] port gigabitethernet 1/0/3
[Device-vlan30] quit
```

Create VLAN-interface 30, and assign IP address 10.1.3.1/24 to it.

```
[Device] interface vlan-interface 30
[Device-Vlan-interface30] ip address 10.1.3.1 255.255.255.0
```

Enabling ARP blackhole routing

```
<Device> system-view
[Device] arp resolving-route enable
```

Enabling ARP active acknowledgment in strict mode

```
<Device> system-view
[Device] arp active-ack strict enable
```

Disabling gratuitous ARP packet learning

```
<Device> system-view
[Device] undo gratuitous-arp-learning enable
```

Enabling ARP packet rate limit and setting the limit rate

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] arp rate-limit 50
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] arp rate-limit 50
[Device-GigabitEthernet1/0/2] quit
```

Configuring ARP source suppression

```
[Device] arp source-suppression enable
[Device] arp source-suppression limit 40
```

Configuring source MAC-based ARP attack detection

The following switch series in R661x version do not support this feature:

- S6520X-HI switch series.
- S6520X-EI switch series.
- S6520X-SI switch series.
- S6520-SI switch series.
- S5000-EI switch series.
- MS4600 switch series.
- S5560X-EI switch series.
- S5560X-HI switch series.
- S5500V2-EI switch series.
- MS4520V2 switch series.
- ES5500 switch series.

Enable source MAC-based ARP attack detection, and specify the handling method as filter.

```
<Device> system-view
[Device] arp source-mac filter
```

Set the threshold to 30.

```
[Device] arp source-mac threshold 30
```

Set the lifetime for ARP attack entries to 60 seconds.

```
[Device] arp source-mac aging-time 60
```

Exclude MAC address 0c68-d691-0606 from this detection.

```
[Device] arp source-mac exclude-mac 0c68-d691-0606
```

Verifying the configuration

Display the current configuration information about ARP source suppression. ARP source suppression is enabled and the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds is 40.

```
<Device> display arp source-suppression
 ARP source suppression is enable
 Current suppression limit: 40
```

Display the ARP attack entries for Host D when Host D sends more than 30 ARP requests to the device within 5 seconds. The command output shows that an ARP attack entry has been generated for Host D. With this ARP attack entry, the device cannot create ARP entries for Host D.

```
<Device> display arp source-mac slot 1
Source-MAC     VLAN ID Interface               Aging time (sec) Packets dropped
0c68-be82-0206 20      GE1/0/2                 10               244
<Device> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
```

Display the ARP attack entries when Host B sends more than 30 ARP requests to the device within 5 seconds. No ARP attack entries for Host B exist, so the device can create ARP entries for Host B.

```
<Device> display arp source-mac slot 1
Source-MAC     VLAN ID Interface               Aging time (sec) Packets dropped
<Device> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
10.1.1.3        0c68-d691-0606 10            GE1/0/1                 1197  D
```

Stop sending ARP packets from Host D to the device and wait the lifetime of the ARP attack entry for Host D expires. Then, configure Host D to send ARP packets to the device. Use the following command to display ARP entries on the device. The output shows that the device has created ARP entries for Host D.

```
<Device> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
10.1.1.3        0c68-d691-0606 10            GE1/0/1                 944   D
10.1.2.3        0c68-be82-0206 20            GE1/0/2                 1195  D
```

Configuration files

IMPORTANT:

Support for the **`port link-mode bridge`** command depends on the device model.

```
#
vlan 1

#
```

```
vlan 10

#
vlan 20

#
vlan 30

#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0

#
interface Vlan-interface20
 ip address 10.1.2.1 255.255.255.0

#
interface Vlan-interface30
 ip address 10.1.3.1 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 arp rate-limit 50

#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 arp rate-limit 50

#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
 undo gratuitous-arp-learning enable
 arp source-mac filter
 arp source-mac aging-time 60
 arp source-mac exclude-mac 0c68-d691-0606
 arp active-ack strict enable
 arp source-suppression enable
 arp source-suppression limit 40
```

Contents

Introduction

This document provides examples for upgrading software on an IRF fabric.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IRF.

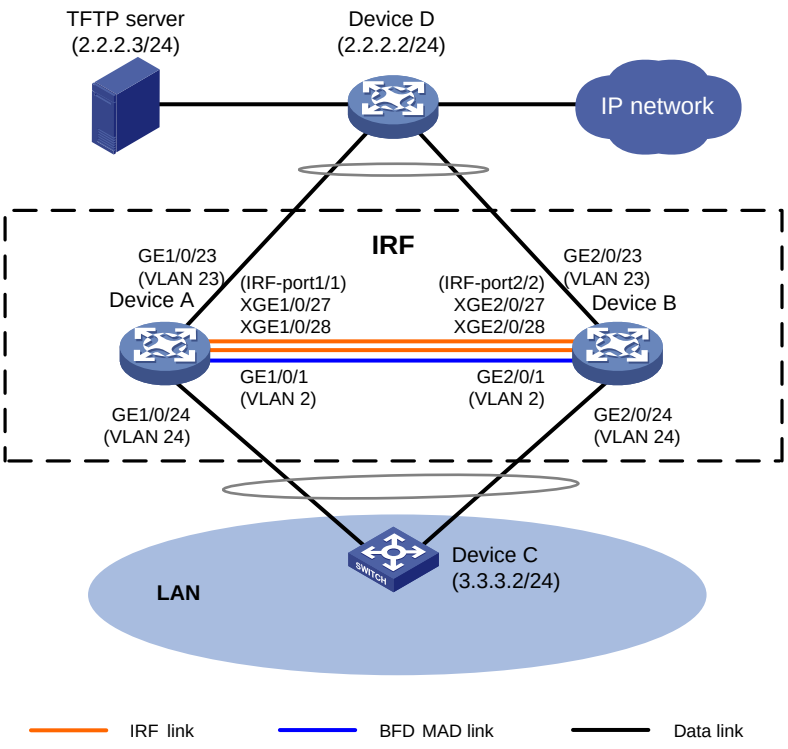
Example: Upgrading software on an IRF fabric

Network configuration

As shown in Figure 1, Device A and Device B have set up an IRF fabric. Device A is the master device and its member ID is 1, and Device B is the standby device and its member ID is 2. BFD MAD is used for multi-active collision detection.

The current software version of the IRF fabric is R2432p06. Upgrade the software version to R2720. After software upgrade, Device A is still the master device.

Figure 1 Network diagram



Analysis

H3C devices support upgrade methods as shown in Table 1. In this example, software is upgraded from the CLI by using the boot loader method. To reduce service interruption time during the upgrade process, IRF split and IRF merge will be performed during the upgrade process.

Table 1 Software upgrade methods

Upgrade method	Software types	Remarks
Upgrading from the CLI by using the boot loader method	• BootWare image • Comware images (excluding incremental patches)	This method is disruptive. You must reboot the entire device to complete the upgrade. All models support this method.
Performing an ISSU from the CLI	Comware images	This method enables a software upgrade with a minimum amount of downtime. Some models support this method.
Upgrading from the BootWare menu	• BootWare image • Comware images	Use this method when the device cannot start up correctly. To use this method, first connect to the console port and power cycle the device. Then, press **Ctrl+B** at prompt to access the BootWare menu. For more information about upgrading software from the BootWare menu, see the release notes for the software version. All models support this method.

To upgrade software on an IRF fabric from the CLI by using the boot loader method:

1. Shut down all uplink and downlink service interfaces on the master device (Device A) in bulk to switch traffic from Device A to Device B. To enter interface range view, use the **`interface range`** command.
2. Upgrade software on Device A from the CLI by using the boot loader method and reboot the device. During the reboot, shut down IRF physical interfaces Ten-GigabitEthernet 2/0/27 and Ten-GigabitEthernet 2/0/28 on Device B. The IRF fabric splits.

CAUTION:

To prevent configuration loss from affecting interface status and causing IRF merge failure or service traffic interruption, do not save the running configuration on any IRF member device when the IRF fabric splits.

NOTE:

To split an IRF fabric, you can remove cables from IRF physical interfaces or shut down all IRF physical interfaces on the standby device. The latter method is simpler. In this example, the latter method is used.

3. Shut down all uplink and downlink service interfaces on the standby device (Device B) in bulk. Bring up all uplink and downlink service interfaces on Device A to switch service traffic back to Device A.
4. Upgrade software on Device B. After Device B reboots, Device A and Device B automatically form an IRF fabric.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series	Release 63xx

Hardware	Software version
S5130S-SI switch series S5130S-LI switch series	
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

Whole upgrade process

As a best practice to discover, locate, and analyze issues in time, record all operations during the whole upgrade process.

Before IRF software upgrade

- Make sure all member devices and cards are in stable state. For this purpose, execute the **`display system stable state`** command and verify that the value for the **State** field is **Stable**. If a member device or card is not in stable state, identify the reason. Do not upgrade software on the IRF fabric unless all member devices and cards are in stable state.
- Prepare scripts in advance for shutting down and bringing up uplink and downlink service interfaces. To prevent omission of service interfaces from resulting in exceptions in the upgrade process, make sure the scripts contain all service interfaces on the IRF fabric.

During IRF software upgrade

- First upgrade software for the master device. Make sure the master device has a higher member priority than the standby device.
- To avoid configuration loss, do not save the running configuration on any IRF member device when the IRF fabric splits.
- After the master device starts up after software upgrade, make sure all member devices and cards are running correctly. Use the **`display interface`** command to verify that all interfaces are displayed, and then wait for 2 minutes before you move to the next step.
- After the standby device reboots, reconnect IRF links before the standby device finishes restartup. If you reconnect IRF links after the standby device finishes restartup, the standby device must reboot again to complete IRF merge with the master device.

After IRF software upgrade

- Make sure all member devices and cards are in stable state. For this purpose, execute the **`display system stable state`** command and verify that the value for the **State** field is **Stable**.
- Verify that all services on the IRF fabric are running correctly. If a service cannot run correctly, locate and resolve the issue as soon as possible.

Prerequisites

1. Configure NSR settings on the IRF fabric:

During the upgrade process, master/standby switchover will occur. If the IRF fabric runs routing protocols, for example, BGP and OSPF, the switchover issue might cause routing neighbor flapping and affect packet forwarding. For high availability, configure NSR for routing protocols. Before upgrading software on the IRF fabric, configure NSR settings and save the configuration. In this example, OSPF NSR and BGP NSR are configured for illustration.

Enable NSR for OSPF process 100.

```
<IRF> system-view
[IRF] ospf 100
[IRF-ospf-100] non-stop-routing
[IRF-ospf-100] display ospf non-stop-routing status

          OSPF Process 100 with Router ID 1.1.1.1
```

```
                Non Stop Routing information

 Non Stop Routing capability : Enabled
 Upgrade phase : Normal
[IRF-ospf-100] quit
[IRF] quit
```

Enable NSR for BGP process 100.

```
[IRF] bgp 100
[IRF-bgp-default] non-stop-routing
[IRF-bgp-default] display bgp non-stop-routing status

 BGP NSR status: Ready
 Location of preferred standby process: Slot 2
 TCP NSR status: Ready
[IRF-bgp-default] quit
[IRF-bgp] quit
```

2. Verify that the master device is assigned a higher member priority than the standby device. The higher the priority value, the higher the priority to be the master device. In this example, set the member priority of Device A to 32.

```
[IRF] irf member 1 priority 32
```

3. Check single-armed service links.

IRF split will occur during the upgrade process. In addition, you need to shut down all service interfaces on one member device. For high availability, deploy physical links dual-homed to both member devices for each uplink device and downlink device. That is, connect Device D to both Device A and Device B, and connect Device C to both Device A and Device B. If single-armed services exist, service access exception will occur during the upgrade process. As a best practice, add backup links for single-armed services.

4. Check IRF status and collect information:

Before the upgrade process, you must check the device status, HA status, IRF status, and MAD status.

IMPORTANT:

Make sure all member devices and cards are in stable state. If a member device or card is not in stable state, identify the reason. Do not upgrade software on an IRF fabric unless all member devices and cards are in stable state.

Display device information.

```
[IRF] display device
Slot Type             State    Subslot  Soft Ver            Patch Ver
1    S5560X-30C-PWR-EIMaster   0        2432p06             None
2    S5560X-30C-PWR-EIStandby  0        2432p06             None
```

Display system stable status.

```
[IRF] display system stable state
System state     : Stable
Redundancy state : Stable
  Slot    CPU    Role       State
  1       0      Active     Stable
  2       0      Standby    Stable
```

Display brief information about system stability and status, including CPU running status, redundancy status, and NSR status.

```
[IRF] display system stable state summary
System state      : Stable
Redundancy state  : Stable
NSR     state     : Ready
```

Display IRF information.

```
<IRF> display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        f010-90db-7402  ---
   2        Standby 1         f010-90db-0204  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 0000-0001-0002
 Auto upgrade               : yes
 Mac persistent             : 12 min
 Domain ID                  : 0
```

Display IRF configuration on all IRF member devices.

```
<IRF> display irf configuration
 MemberID NewID    IRF-Port1                     IRF-Port2
 1        1        Ten-GigabitEthernet1/0/27     disable
                   Ten-GigabitEthernet1/0/28
 2        2        disable                       Ten-GigabitEthernet2/0/27
                                                  Ten-GigabitEthernet2/0/28
```

Display IRF link information.

```
<IRF> display irf link
Member 1
 IRF Port  Interface                             Status
 1         Ten-GigabitEthernet1/0/27             UP
           Ten-GigabitEthernet1/0/28             UP
 2         disable                               --
Member 2
 IRF Port  Interface                             Status
 1         disable                               --
 2         Ten-GigabitEthernet2/0/27             UP
           Ten-GigabitEthernet2/0/28             UP
```

Display IRF topology information.

```
<IRF> display irf topology
                            Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
 MemberID    Link       neighbor      Link       neighbor    Belong To
 2           DIS        ---           UP         1           f010-90db-7402
 1           UP         2             DIS        ---         f010-90db-7402
```

Display detailed MAD information.

```
<IRF> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
```

```
Excluded ports (system-configured):
  IRF physical interfaces:
    Ten-GigabitEthernet1/0/27
    Ten-GigabitEthernet1/0/28
    Ten-GigabitEthernet2/0/27
    Ten-GigabitEthernet2/0/28
  BFD MAD interfaces:
    Vlan-interface2
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface2
  MAD status                  : Normal
  Member ID   MAD IP address       Neighbor   MAD status
  1           192.168.2.1/24       2          Normal
  2           192.168.2.2/24       1          Normal
```

Display BFD session information.

```
[IRF] display bfd session
 Total Sessions: 1     Up Sessions: 1     Init mode: Active

 IPv4 session working in control packet mode:

 LD/RD           SourceAddr      DestAddr        State    Holdtime    Interface
 32833/0         192.168.2.1     192.168.2.2     Down        /        Vlan2
```

5. Verify that the IRF fabric is running correctly, and collect status information, including status information for protocols, ports, and table entries, for comparing the information with the information collected after the upgrade:

Display system version information.

```
<IRF> display version
H3C Comware Software, Version 7.1.070, Release 2432p06
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5560X-30C-PWR-EI uptime is 4 weeks, 2 days, 22 hours, 3 minutes
Last reboot reason : User reboot

Boot image: flash:/cmw710-system-r2432p06.bin
Boot image version: 7.1.070, Release 2432p06
  Compiled Sep 29 2021 11:00:00
System image: flash:/cmw710-system-r2432p06.bin
System image version: 7.1.070, Release 2432p06
  Compiled Sep 29 2021 11:00:00
...
```

Display the running configuration.

```
<IRF> display current-configuration
#
 version 7.1.070, Release 2432p06
#
 sysname IRF
#
```

```
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
 irf member 2 priority 1
#
ospf 100
 non-stop-routing
#
...
```

Display brief interface information.

```
<IRF> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP        Description
InLoop0              UP   UP(s)    --
MGE0/0/0             DOWN DOWN     --
NULL0                UP   UP(s)    --
REG0                 UP   --       --
Vlan2                UP   UP       192.168.2.1

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed     Duplex Type PVID Description
GE1/0/1               UP   1G(a)     F(a)   A    2
GE1/0/2               DOWN auto      A      A    1
GE1/0/3               DOWN auto      A      A    1
...
```

Display ARP entries.

```
<IRF> display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
2.2.2.2         6451-c3f1-0302 20            BAGG1                   941   D
3.3.3.2         6451-ccf3-0402 30            BAGG2                   1020  D
```

Display MAC address table information.

```
<IRF> display mac-address
MAC Address      VLAN ID    State           Port/Nickname           Aging
a442-f6d0-9344   2          Learned         GE1/0/1                 Y
6451-c3f1-0302   23         Learned         BAGG1                   Y
6451-ccf3-0402   24         Learned         BAGG2                   Y
```

Display information about OSPF neighbors. In this example, static routing is used. The command does not display any information.

```
<IRF> display ospf peer
```

Display routing table information.

```
<IRF> display ip routing-table

Destinations : 21       Routes : 21

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  60  0           2.2.2.2         Vlan23
1.1.1.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.0/24         Direct  0   0           2.2.2.1         Vlan23
2.2.2.0/32         Direct  0   0           2.2.2.1         Vlan23
2.2.2.1/32         Direct  0   0           127.0.0.1       InLoop0
2.2.2.255/32       Direct  0   0           2.2.2.1         Vlan23
3.3.3.0/24         Direct  0   0           3.3.3.1         Vlan24
3.3.3.0/32         Direct  0   0           3.3.3.1         Vlan24
3.3.3.1/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.255/32       Direct  0   0           3.3.3.1         Vlan24
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.2.0/24     Direct  0   0           192.168.2.1     Vlan2
192.168.2.0/32     Direct  0   0           192.168.2.1     Vlan2
192.168.2.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.2.255/32   Direct  0   0           192.168.2.1     Vlan2
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Display detailed information about aggregation groups.

```
<IRF> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
  GE1/0/10(R)      S       32768    1
  GE2/0/10         S       32768    1

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key
```

```
  GE1/0/23          S       32768    2
  GE2/0/23(R)       S       32768    2
```

6. Back up the main next-startup configuration file:

Save the running configuration to the main next-startup configuration file.

```
<IRF> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 0 commands and
deletes 0 commands.
If you want to see the configuration differences, please cancel this operation, and
then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

Display the names of the current startup configuration file and the next-startup configuration files.

```
<IRF> display startup
MainBoard:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

Back up next-startup configuration file **startup.cfg**.

```
<IRF> tftp 2.2.2.3 put startup.cfg
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  8128    0     0  100  8128      0   170k --:--:-- --:--:-- --:--:--  233k

<IRF>
```

7. Verify that the member devices have sufficient storage space to store the new startup image file:

On Device A, display information about files and directories in the current directory.

```
<IRF> dir
Directory of flash:
   1 -rw-      220684 Nov 15 2021 17:37:48   defaultfile.zip
   2 drw-           - Jan 01 2021 00:01:33   diagfile
...
```

```
554288 KB total (228880 KB free)
```

On Device B, display information about files and directories in the current directory.

```
<IRF> dir slot2#flash:/
Directory of flash:
   1 -rw-      220684 Nov 15 2021 17:37:48   defaultfile.zip
   2 drw-           - Jan 01 2011 00:01:33   diagfile
...

554288 KB total (221104 KB free)
```

8. Upload the new startup image file and validate the file:

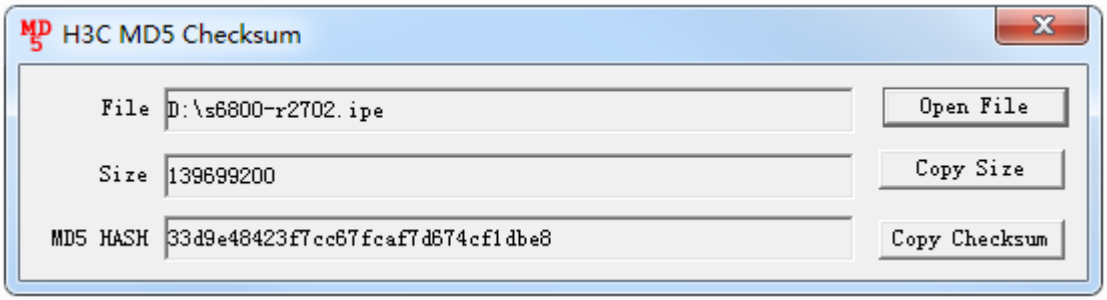
Upload image file **r2702.ipe** to Device A, and verify that the size of the uploaded file on Device A is the same as that of the officially released one. If the file sizes are different, upload the file again.

```
<IRF> tftp 2.2.2.3 get r2702.ipe
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  133M  100  133M    0     0   180k      0  0:12:33  0:12:33 --:--:--  177k
Writing file...Done.
<IRF> dir r2702.ipe
Directory of flash:
   25 -rw-   139699200 Nov 19 2021 12:07:56   r2702.ipe

524288 KB total (167504 KB free)
```

Use MD5 digest to validate the new startup image file. The file is valid if the digest calculated by using the **md5sum** command is the same as the MD5 digest published when the image file was released or the same as the file's digest generated by using an MD5 tool.

```
<IRF> md5sum r2702.ipe
MD5 digest:
33d9e48423f7cc67fcaf7d674cf1dbe8
```

Figure 2 Using an MD5 tool to generate a digest



9. Copy the new startup image file to Device B for backup.

```
<IRF> copy r2702.ipe slot2#flash:/
Copy flash:/r2702.ipe to slot2#flash:/r2702.ipe? [Y/N]:y
Copying file flash:/r2702.ipe to slot2#flash:/r2702.ipe.................. Done.
```

Procedures

Specifying the new startup image file and verifying the configuration

Specifying file **r2702.ipe** as the main startup image file.

```
<IRF> boot-loader file flash:/r2702.ipe all main
Verifying the file flash:/r2702.ipe on slot 1.................................
.................Done.
H3C S5560X-30C-PWR-EI images in IPE:
  cmw710-boot-r2702.bin
  cmw710-system-r2702.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file cmw710-boot-r2702.bin to
flash:/cmw710-boot-r2702.bin.........................Done.
Decompressing file cmw710-system-r2702.bin to
flash:/cmw710-system-r2702.bin.....................................................
.....................................................................................
.........................Done.
Verifying the file flash:/cmw710-boot-r2702.bin on slot 1........Done.
Verifying the file flash:/cmw710-system-r2702.bin on slot
1.............................................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
Loading.....................................................Done.
Loading.....................................................................
.....................................................................................
.....................................................................Done
.
Verifying the file flash:/cmw710-boot-r2702.bin on slot 2....Done.
Verifying the file flash:/cmw710-system-r2702.bin on slot 2..................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
Decompression completed.
Do you want to delete flash:/5560.ipe now? [Y/N]:n
```

Verify that file **r2702.ipe** has been specified as the main startup image file on all slots.

```
<IRF> display boot-loader
Software images on slot 1:
Current software images:
  flash:/cmw710-boot-r2432p06.bin
  flash:/cmw710-system-r2432p06.bin
Main startup software images:
  flash:/cmw710-boot-r2702.bin
  flash:/cmw710-system-r2702.bin
Backup startup software images:
  flash:/cmw710-boot-r2432p06.bin
  flash:/cmw710-system-r2432p06.bin
Software images on slot 2:
Current software images:
  flash:cmw710-boot-r2432p06.bin
```

```
  flash:/cmw710-system-r2432p06.bin
Main startup software images:
  flash:/cmw710-boot-r2702.bin
  flash:/cmw710-system-r2702.bin
Backup startup software images:
  flash:/cmw710-boot-r2432p06.bin
  flash:/cmw710-system-r2432p06.bin
```

Disabling MAD (BFD MAD in the example)

Disable MAD and remove cables from the interfaces used for MAD. In this example, VLAN-interface 2 is used for BFD MAD.

```
<IRF> system-view
[IRF] interface vlan-interface 2
[IRF-Vlan-interface2] undo mad bfd enable
[IRF-Vlan-interface2] display this
#
interface Vlan-interface2
#
return
```

Shutting down service interfaces on the master device and saving the configuration

Shut down all uplink and downlink interfaces on Device A. Do not shut down IRF physical interfaces and the interfaces used for BFD MAD on Device A.

```
[IRF] interface range name yewu interface gigabitethernet 1/0/2 to gigabitethernet 1/0/22
ten-gigabitethernet 1/0/25 to ten-gigabitethernet 1/0/26
[IRF] interface range name yewu
[IRF-if-range-yewu] shutdown
[IRF-if-range-yewu] quit
[IRF] quit
```

On Device D and Device C, ping each other. If the ping operations succeed, Device C and Device D are reachable. If the ping operations fail, locate and resolve the communication failure issue. (Details not shown.)

Verify that all services have been switched from Device A to Device B. (Details not shown.)

Save the running configuration.

```
<IRF> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 0 commands and deletes
0 commands.
If you want to see the configuration differences, please cancel this operation, and then
use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

Rebooting the master device and splitting the IRF fabric

Reboot the master device (Device A).

```
<IRF> reboot slot 1
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait.........
```

Shut down IRF physical interfaces Ten-GigabitEthernet 2/0/27 and Ten-GigabitEthernet 2/0/28 on Device B to cause IRF split.

CAUTION:

The IRF fabric splits after you shut down all IRF physical interfaces on Device B. To prevent configuration loss from affecting interface status and causing IRF merge failure or service traffic interruption, do not save the running configuration on the master device (Device A) when the IRF fabric splits.

```
<IRF> system-view
[IRF] interface range name irf-port interface ten-gigabitethernet 2/0/27 to
ten-gigabitethernet 2/0/28
[IRF-if-range-irf-port] shutdown
```

Shutting down service interfaces on the standby device and bringing up service interfaces on the master device

IMPORTANT:

To reduce the service interruption time, shorten the operation time as much as possible. As a best practice, prepare the required command lines in advance and copy and paste the command lines to the devices.

After Device A finishes startup, verify that all interfaces are displayed.

```
<IRF> display interface
```

Wait for about 2 minutes for forwarding entry convergence on Device A.

Verify that Device A is stable.

```
<IRF> display system stable state
System state     : Stable
Redundancy state : No redundancy
  Slot    CPU    Role       State
  1        0          Active     Stable
```

Log in to Device B and shut down all service interfaces on the device. Do not shut down IRF physical interfaces and the interfaces used for BFD MAD.

```
<IRF> system-view
[IRF] interface range name yewu-2 interface gigabitethernet 2/0/2 to gigabitethernet
2/0/22 ten-gigabitethernet 2/0/25 to ten-gigabitethernet 2/0/26
```

```
[IRF] interface range name yewu-2
[IRF-if-range-yewu-2] shutdown
```

Log in to Device A and bring up all service interfaces on the device.

```
<IRF> system-view
[IRF] interface range name yewu
[IRF-if-range-yewu] undo shutdown
```

Rebooting the standby device

Verify that services have been switched back to Device A. (Details not shown.)

,Log in to Device B and reboot Device B.

```
<IRF> reboot slot 2
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait.........
```

After Device B reboots, it acts as a standby device to complete IRF merge with Device A.

Checking the environment after IRF software upgrade

1. Check IRF status and services:

   # After Device B reboots, check IRF status and service status, collect status information, and compare the status information with that before the upgrade process. If the status information is inconsistent before and after upgrade, locate and resolve the issue.

   ```
   [IRF] display system stable state
   [IRF] display irf
   [IRF] display irf configuration
   [IRF] display irf link
   [IRF] display irf topology
   ```

2. Enable MAD and verify the configuration.

   ```
   [IRF] interface vlan-interface 2
   [IRF-Vlan-interface2] mad bfd enable
   [IRF-Vlan-interface2] mad ip address 192.168.2.1 24 member 1
   [IRF-Vlan-interface2] mad ip address 192.168.2.2 24 member 2
   [IRF-Vlan-interface2] quit
   [IRF] display mad verbose
   Multi-active recovery state: No
   Excluded ports (user-configured):
   Excluded ports (system-configured):
     IRF physical interfaces:
   ```

```
    Ten-GigabitEthernet1/0/27
    Ten-GigabitEthernet1/0/28
    Ten-GigabitEthernet2/0/27
    Ten-GigabitEthernet2/0/28
  BFD MAD interfaces:
    Vlan-interface2
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface2
  MAD status                 : Normal
  Member ID   MAD IP address       Neighbor   MAD status
  1           192.168.2.1/24       2          Normal
  2           192.168.2.2/24       1          Normal
```

3. Delete unused settings as needed and save the configuration.

```
[IRF] undo interface range yewu
[IRF] undo interface range yewu-2
[IRF] save
```

4. Check the device status, collect device status information, and compare the device status with that before the upgrade process. If the device status information is inconsistent before and after upgrade, locate and resolve the issue.

```
<IRF> display version
<IRF> display current-configuration
<IRF> display interface brief
<IRF> display arp
<IRF> display mac-address
<IRF> displayplay ospf peer
<IRF> display ip routing-table
<IRF> display link-aggregation verbose
```

Verifying the configuration

Display IRF version information. Verify that the software version has been upgraded from R2432p06 to R2720.

```
<IRF> display version
H3C Comware Software, Version 7.1.070, Release 2720
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5560X-30C-PWR-EI uptime is 4 weeks, 5 days, 14 hours, 32 minutes
Last reboot reason : User reboot

Boot image: flash:/cmw710-boot-r2720.bin
Boot image version: 7.1.070, Release 2720
  Compiled Sep 29 2021 11:00:00
System image: flash:/cmw710-system-r2720.bin
System image version: 7.1.070, Release 2720
  Compiled Sep 29 2021 11:00:00
```

```
Slot 1:
Uptime is 4 weeks,5 days,14 hours,32 minutes
S5560X-30C-PWR-EI with 1 RMI XLS408 Processor
BOARD TYPE:          S5560X-30C-PWR-EI
DRAM:                2048M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.A
FPGA Version:        NONE
Bootrom Version:     158
CPLD 1 Version:      002
CPLD 2 Version:      001
Release Version:     H3C S5560X-30C-PWR-EI-2720
Patch Version:       None
Reboot Cause:        UserReboot
[SubSlot 0] 48XGT+6QSFP Plus
```

Contents

Introduction

This document provides examples for replacing an IRF member device with a new device.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of IRF.

Example: Replacing an IRF member device with a new device

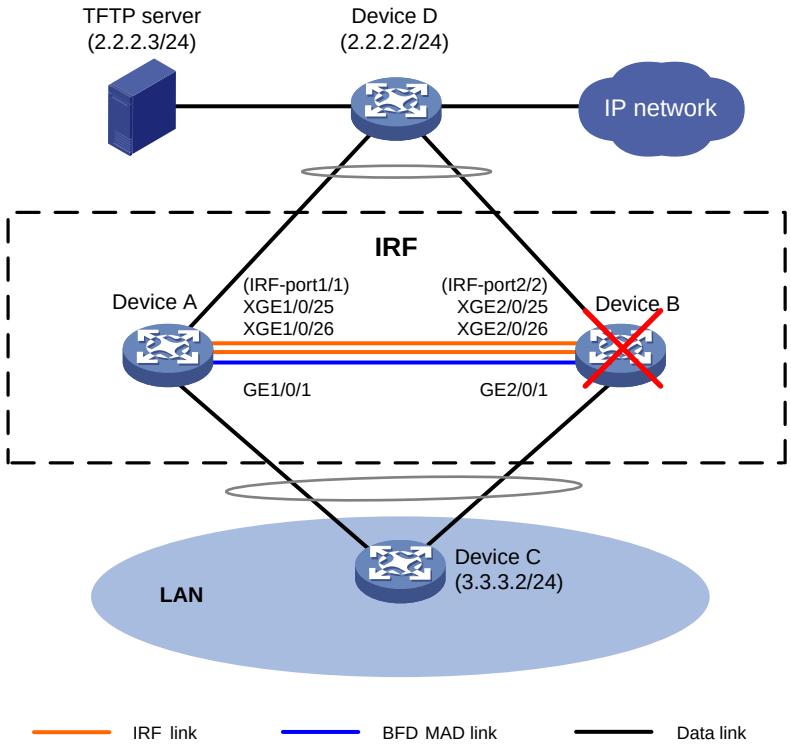
In this example, the IRF fabric does not split. Because the standby device fails, you need to replace the standby device with a new device. During the replacement, the IRF fabric will split. The procedures in this example are also applicable to master device replacement in scenarios where the master device fails when the IRF fabric is integrated.

Network configuration

As shown in Figure 1, Device A and Device B have set up an IRF fabric. Device A is the master device and its member ID is 1, and Device B is the standby device and its member ID is 2. BFD MAD is used for multi-active collision detection.

Device B fails when the IRF fabric is integrated. Replace Device B with a new device.

Figure 1 Network diagram



Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Release 8005 and later, Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch	Release 63xx

Hardware	Software version
MS4520V2-24TP switch	
S6520X-HI switch series S6520X-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except the S5500V3-24P-SI and S5500V3-48P-SI switches)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx
S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series	Release 63xx

Hardware	Software version
S5000X-EI switch series	
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch	Release 6810 and later

Restrictions and guidelines

Change the IRF member ID of the new device in advance and reboot the device for the change to take effect.

Prepare scripts in advance for shutting down or bringing up the uplink and downlink service interfaces on Device B. To prevent omission of service interfaces from resulting in exceptions in the replacement process, make sure the scripts contain all service interfaces on Device B.

To avoid configuration loss, do not save the running configuration on any IRF member device when the IRF fabric splits.

After the IRF fabric recovers, make sure all member devices are running correctly. Use the **`display interface brief`** command to verify that all interfaces are displayed, and then wait for 2 minutes before you move to the next step.

As a best practice to discover, locate, and analyze issues in time, record all operations during the whole replacement process. Login software, for example, HyperTerminal and PuTTY, supports session recording. The software can automatically record all user operations and save the operations to a .txt file. If the login software does not support session recording, you must manually record all operations.

Prerequisites

1. Configure NSR settings on the IRF fabric:

   During the replacement, process-level active/standby switchover might occur for routing protocols such as BGP and OSPF. This issue causes routing neighbor flapping and affects

packet forwarding. For high availability, configure NSR for routing protocols. Before replacing Device B, configure NSR settings and save the configuration. In this example, OSPF NSR and BGP NSR are configured for illustration.

Enable NSR for OSPF process 100.

```
<IRF> system-view
[IRF] ospf 100
[IRF-ospf-100] non-stop-routing
[IRF-ospf-100] display ospf non-stop-routing status

         OSPF Process 100 with Router ID 1.1.1.1
                 Non Stop Routing information

 Non Stop Routing capability : Enabled
 Upgrade phase : Normal
[IRF-ospf-100] quit
[IRF] quit
```

Enable NSR for BGP process 100.

```
[IRF] bgp 100
[IRF-bgp-default] non-stop-routing
[IRF-bgp-default] display bgp non-stop-routing status

 BGP NSR status: Ready
 Location of preferred standby process: Slot 2
 TCP NSR status: Ready
[IRF-bgp-default] quit
[IRF-bgp] quit
[IRF] quit
```

2. Examine whether Device B has single-armed service links.

Single-armed service links refer to links connected only to one IRF member device in an IRF fabric. They do not connect to other IRF member devices in the IRF fabric. If single-armed service links exist, traffic interruption will occur during the replacement process. To avoid traffic interruption, add backup links for the single-armed links.

3. Check IRF status and collect information:

Before the replacement, you must check the device status, HA status, IRF status, and MAD status.

IMPORTANT:

Make sure all member devices except Device B are in stable state. If a member device is not in stable state, identify the reason. Do not replace Device B with a new device unless other member devices are all in stable state.

Display device information.

```
<IRF> display device
Slot Type              State    Subslot  Soft Ver            Patch Ver
1    S5560X-30C-PWR-EI Master   0        S5560X-6530P01      None
2    S5560X-30C-PWR-EI Standby  0        S5560X-6530P01      None
```

Display system stable status.

```
<IRF> display system stable state
System state     : Stable
Redundancy state : Stable
```

```
  Slot    CPU    Role       State
  1       0      Active     Stable
  2       0      Standby    Stable
```

Display brief information about system stability and status, including CPU running status, redundancy status, and NSR status.

```
<IRF> display system stable state summary
System state      : Stable
Redundancy state  : Stable
NSR     state     : Ready
```

Display IRF information.

```
<IRF> display irf
MemberID    Role    Priority  CPU-Mac         Description
*+1         Master  1         f010-90db-7402  ---
  2         Standby 1         f010-90db-8100  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: ae05-0607-eaaa
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
```

Display IRF configuration on all IRF member devices.

```
<IRF> display irf configuration
 MemberID NewID    IRF-Port1                     IRF-Port2
 1        1        Ten-GigabitEthernet1/0/25     disable
                   Ten-GigabitEthernet1/0/26
 2        2        disable                       Ten-GigabitEthernet2/0/25
                                                  Ten-GigabitEthernet2/0/26
```

Display IRF link information.

```
<IRF> display irf link
Member 1
 IRF Port  Interface                             Status
 1         Ten-GigabitEthernet1/0/25             UP
           Ten-GigabitEthernet1/0/26             UP
 2         disable                               --
Member 2
 IRF Port  Interface                             Status
 1         disable                               --
 2         Ten-GigabitEthernet2/0/25             UP
           Ten-GigabitEthernet2/0/26             UP
```

Display IRF topology information.

```
<IRF> display irf topology
                             Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
 MemberID    Link       neighbor      Link       neighbor    Belong To
 2           DIS        ---           UP         1           f010-90db-7402
```

```
 1           UP         2             DIS        ---         f010-90db-7402
```

Display detailed MAD information.

```
<IRF> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  IRF physical interfaces:
    Ten-GigabitEthernet1/0/25
    Ten-GigabitEthernet1/0/26
    Ten-GigabitEthernet2/0/25
    Ten-GigabitEthernet2/0/26
  BFD MAD interfaces:
    Vlan-interface2
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface2
  MAD status                  : Normal
  Member ID   MAD IP address       Neighbor   MAD status
  1           192.168.2.1/24       2          Normal
  2           192.168.2.2/24       1          Normal
```

Display BFD session information.

```
<IRF> display bfd session
 Total Sessions: 1     Up Sessions: 0     Init mode: Active

 IPv4 session working in control packet mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 32833/0        192.168.2.1     192.168.2.2     Down        /        Vlan2
```

4. Examine licensing state on the IRF fabric. If Device B has been installed with formal licenses, you must transfer the licenses on Device B to the new device before the replacement process. Alternatively, you can apply for and install new licenses of the same specification for the new device. For more information about license transfer and installation, see the licensing guide for the product. You cannot transfer trial licenses.

```
<IRF> display license
Slot 1:
flash:/license/210235A1XE000000000120200623142526399O3.ak
Feature: OPENXCVR
Product Description: H3C Open Optical Transceiver Module Support License for
40G/10G(or Lower) Fixed-Port Campus Switches
Registered at: 2021-12-10 06:03:27
License Type: Permanent
Current State: In use

Slot 2:
flash:/license/210235A1XE000000000120200623142526311l0.ak
Feature: OPENXCVR
Product Description: H3C Open Optical Transceiver Module Support License for
40G/10G(or Lower) Fixed-Port Campus Switches
```

```
Registered at: 2021-12-10 06:03:27
License Type: Permanent
Current State: In use
```

5. Verify that the IRF fabric is running correctly, and collect status information, including status information for protocols, ports, and table entries, for comparing the information with the information collected after the replacement:

Display system version information.

```
<IRF> display version
```

Display the running configuration.

```
<IRF> display current-configuration
```

Display brief interface information.

```
<IRF> display interface brief
```

Display ARP entries.

```
<IRF> display arp
```

Display MAC address table information.

```
<IRF> display mac-address
```

Display information about OSPF neighbors.

```
<IRF> display ospf peer
```

Display routing table information.

```
<IRF> display ip routing-table
```

Display detailed information about aggregation groups.

```
<IRF> display link-aggregation verbose
```

Display traffic rate statistics for interfaces in up state within the most recent statistics polling interval.

```
<IRF> display counters rate inbound interface
```

6. Back up the main next-startup configuration file:

Save the running configuration to the main next-startup configuration file.

```
<IRF> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 0 commands and deletes 0 commands.
If you want to see the configuration differences, please cancel this operation, and then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

Display the names of the current startup configuration file and the next-startup configuration files.

```
<IRF> display startup
MainBoard:
 Current startup saved-configuration file: NULL
```

```
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

Back up next-startup configuration file **startup.cfg**.

```
<IRF> tftp 2.2.2.3 put startup.cfg
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  8128    0     0  100  8128      0   170k --:--:-- --:--:-- --:--:--  233k

<IRF>
```

7. Prepare the new device:

a. Verify that the new device has the same model as the old device and runs the same version of software as the IRF fabric. If the new device runs a version of software different than the IRF fabric, upgrade the software on the new device.

```
<newDeviceB> display version
H3C Comware Software, Version 7.1.070, Release 6530P01
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C S5560X-30C-PWR-EI uptime is 0 weeks, 0 days, 17 hours, 19 minutes
Last reboot reason : User reboot
...
```

b. Verify that the new device has the same settings for some parameters as Device A. The parameters include the system operating mode and the maximum number of ECMP routes. The parameter requirements vary by device model. For more information about the configuration restrictions and guidelines, see IRF in *Virtual Technologies Configuration Guide* for the device.

c. Change the IRF member ID of the new device to 2, the same as the old device.

```
[newDeviceB] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss.
Continue?[Y/N]:y
[newDeviceB] quit
```

d. Save the running configuration and reboot the new device for the member ID to take effect.

```
<newDeviceB> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 20 commands and
deletes 121 commands.
If you want to see the configuration differences, please cancel this operation,
and then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
```

```
<newDeviceB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait.......
```

e. Configure IRF port bindings. Bind Ten-GigabitEthernet 2/0/25 and Ten-GigabitEthernet 2/0/26 to IRF-port 2/2.

```
<newDeviceB> system-view
[newDeviceB] interface ten-gigabitethernet 2/0/25
[newDeviceB-Ten-GigabitEthernet2/0/25] shutdown
[newDeviceB-Ten-GigabitEthernet2/0/25] quit
[newDeviceB] int ten-gigabitethernet 2/0/26
[newDeviceB-Ten-GigabitEthernet2/0/26] shutdown
[newDeviceB-Ten-GigabitEthernet2/0/26] quit
[newDeviceB] irf-port 2/2
[newDeviceB-irf-port2/2] port group interface ten-gigabitethernet 2/0/25
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[newDeviceB-irf-port2/2] port group interface ten-gigabitethernet 2/0/26
[newDeviceB-irf-port2/2] quit
[newDeviceB] interface ten-gigabitethernet 2/0/25
[newDeviceB-Ten-GigabitEthernet2/0/25] undo shutdown
[newDeviceB-Ten-GigabitEthernet2/0/25] quit
[newDeviceB] int ten-gigabitethernet 2/0/26
[newDeviceB-Ten-GigabitEthernet2/0/26] undo shutdown
[newDeviceB-Ten-GigabitEthernet2/0/26] quit
[newDeviceB] irf-port-configuration active
[newDeviceB] save
```

f. Power off the new device.

Procedures

1. On Device B (the old device), shut down service interfaces and save the configuration:

On Device B, shut down all uplink and downlink service interfaces. Do not shut down IRF physical interfaces Ten-GigabitEthernet 2/0/25 and Ten-GigabitEthernet 2/0/26 and BFD MAD interface GigabitEthernet 2/0/1.

```
[IRF] interface range name yewu interface gigabitethernet 2/0/2 to gigabitethernet
2/0/24 ten-gigabitethernet 2/0/27 to ten-gigabitethernet 2/0/28
[IRF-if-range-yewu] shutdown
[IRF-if-range-yewu] quit
```

On Device D, ping Device C. On Device C, ping Device D. If the ping operations succeed, Device C and Device D are reachable. If the ping operations fail, first locate and resolve the communication failure issue. (Details not shown.)

2. Verify that all services on Device B have been switched over to Device A. (Details not shown.)

3. Save the running configuration.

```
[IRF] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
```

```
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 0 commands and deletes 0 commands.
If you want to see the configuration differences, please cancel this operation, and then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

4. Power off Device B, and then remove cables for IRF physical interfaces and service interfaces.

CAUTION:

The IRF fabric splits after you power off Device B. To avoid configuration loss, do not execute the **save** command on Device A or Device B.

5. Connect IRF physical interfaces to add the new device to the IRF fabric, and power on the new device:

   # Connect IRF physical interfaces Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26 and BFD MAD interface GigabitEthernet 2/0/1, and then power on the new device. The new device and Device A merge into an IRF fabric, and Device A is still the master device.

   # After the new device starts up, execute the following **display** commands to verify that Device B and the IRF fabric are running correctly. The command outputs should be the same as those before the replacement. If the command outputs before and after the replacement are inconsistent, locate and resolve the issue.

   ```
   [IRF] display system stable state
   [IRF] display irf
   [IRF] display irf configuration
   [IRF] display irf link
   [IRF] display irf topology
   [IRF] display mad verbose
   ```

6. After the new device runs stably, connect service interfaces on the new device to uplink and downlink devices and bring up all service interfaces:

   # Verify that the new device is a standby device.

   ```
   [IRF] display device
   ```

   # Verify that all physical interfaces on the new device are displayed.

   ```
   [IRF] display interface
   ```

   # Wait for 2 minutes, and then connect the cables that were connected to service interfaces on the old device to the service interfaces on the new device.

   # Bring up all service interfaces on the new device and verify that all services are running correctly.

   ```
   [IRF] interface range name yewu interface gigabitethernet 2/0/2 to gigabitethernet 2/0/24 ten-gigabitethernet 2/0/27 to ten-gigabitethernet 2/0/28
   [IRF-if-range-yewu] undo shutdown
   [IRF-if-range-yewu] quit
   ```

7. Save the configuration.

   ```
   [IRF] save
   ```

Checking the environment after IRF member replacement

Delete unused settings as needed and save the configuration.

```
[IRF] undo interface range yewu
[IRF] quit
<IRF> save
```

Check the device status, collect device status information, and compare the device status with that before the replacement. If the device status information is inconsistent before and after replacement, locate and resolve the issue.

```
<IRF> display version
<IRF> display current-configuration
<IRF> display interface brief
<IRF> display arp
<IRF> display mac-address
<IRF> display ospf peer
<IRF> display ip routing-table
<IRF> display link-aggregation verbose
<IRF> display counters rate inbound interface
```

Verifying the configuration

Display device information on the IRF fabric. Verify that Device A is the master device and Device B is the standby device.

```
<IRF> display device
Slot Type              State    Subslot  Soft Ver             Patch Ver
1    S5560X-30C-PWR-EI Master   0        S5560X-6530P01       None
2    S5560X-30C-PWR-EI Standby  0        S5560X-6530P01       None
```

Contents

Introduction

This document provides examples for configuring Layer 3 multicast on a DR system attached to multicast sources.

Distributed Resilient Network Interconnect (DRNI) virtualizes two physical devices into one system through multichassis link aggregation. You can configure PIM on a DR system attached to multicast receivers or multicast sources to prevent single points of failure from interrupting multicast forwarding.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of DRNI and Layer 3 multicast.

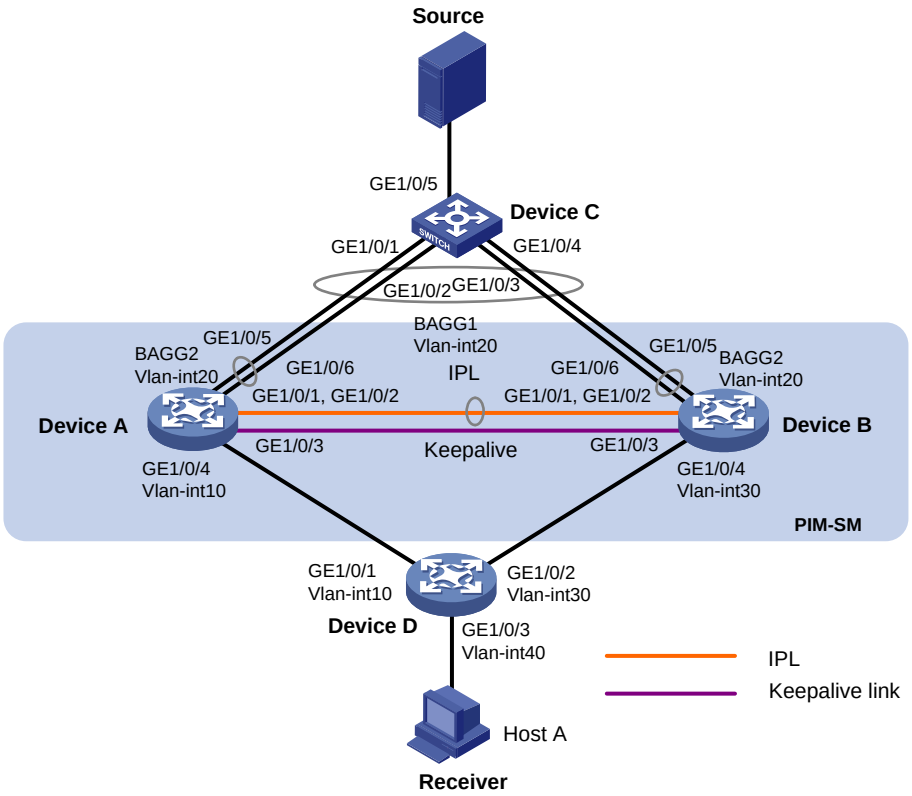
Example: Configuring Layer 3 IPv4 multicast on a DR system attached to multicast sources

Network configuration

As shown in Figure 1:

- OSPF runs on the network.
- VOD streams are sent to receiver hosts in multicast. The receivers of different subnets form stub networks, and a minimum of one receiver host exist on each stub network.
- The entire PIM-SM domain contains only one BSR.
- Device C is a Layer 2 device attached to the multicast source. Switch A and Switch B are virtualized into a DR system, which is connected to Switch C through a multichassis aggregate link. VLAN-interface 20 interfaces on the DR system are the gateway for the multicast source.
- Host A is a multicast data receiver attached to Device D.
- The GigabitEthernet 1/0/3 interfaces on Device A and Device B are excluded from the shutdown action by DRNI MAD to set up the keepalive link.
- A VRRP group is configured on VLAN-interface 20 interfaces. In the VRRP group, Device A is the master.
- DR interfaces on Switch A and Switch B permit packets from VLAN 20 to pass through. PIM is enabled on VLAN-interface 20 of Switch A and Switch B.
- IP multicast routing is enabled on Switch A and Switch B.

Figure 1 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int20	20.0.0.1/24	Device D	Vlan-int10	100.0.0.2/24
	GE1/0/3	200.0.0.1/24		Vlan-int30	30.0.0.2/24
	Vlan-int10	100.0.0.1/24		Vlan-int40	40.0.0.2/24
	Loop0	1.1.1.1			
Device B	Vlan-int20	20.0.0.2/24			
	GE1/0/3	200.0.0.2/24			
	Vlan-int30	30.0.0.1/24			
	Loop0	2.2.2.2			

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 or later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 or later, Release 8106Pxx

Hardware	Software version
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported

Hardware	Software version
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Assigning IP addresses and configuring unicast routing

Assign an IP address and subnet mask to each interface as shown in Figure 1, and configure OSPF on the switches in the PIM-SM domain. (Details not shown.)

Configuring Device A

Configure the DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 1-1-1
[DeviceA] drni system-number 1
[DeviceA] drni system-priority 123
```

Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ip destination 200.0.0.2 source 200.0.0.1
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/3) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface gigabitethernet 1/0/3
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/5] quit
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/6] quit
```

Configure Bridge-Aggregation 1 as a trunk port, assign it to all VLANs, and specify it as the IPP.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan all
[DeviceA-Bridge-Aggregation1] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation1] quit
```

Configure Bridge-Aggregation 2 as a trunk port, and assign it to VLAN 20 and a DR group.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] port link-type trunk
[DeviceA-Bridge-Aggregation2] port trunk permit vlan 20
[DeviceA-Bridge-Aggregation2] port drni group 1
[DeviceA-Bridge-Aggregation2] quit
```

Configure VRRP group 1 on VLAN-interface 20, and set the priority of Device A to 200 for it to be the master in the VRRP group.

```
[DeviceA] vlan 20
[DeviceA-vlan20] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] vrrp vrid 1 virtual-ip 20.0.0.10
[DeviceA-Vlan-interface20] vrrp vrid 1 priority 200
[DeviceA-Vlan-interface20] quit
```

Enable IP multicast routing, enable IGMP and PIM on VLAN-interface 10, and enable PIM-SM on other interfaces as required.

```
[DeviceA] multicast routing
[DeviceA-mrib] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] igmp enable
[DeviceA-Vlan-interface10] pim sm
[DeviceA-Vlan-interface10] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] pim sm
[DeviceA-Vlan-interface20] quit
[DeviceA] interface loopback 0
[DeviceA-LoopBack0] pim sm
[DeviceA-LoopBack0] quit
```

Specify the IP address of Loopback 0 as a C-RP and a C-BSR.

```
[DeviceA] pim
[DeviceA-pim] c-rp 1.1.1.1
[DeviceA-pim] c-bsr 1.1.1.1
[DeviceA-pim] quit
```

Configuring Device B

Configure Device B in the same way you configure Device A. (Details not shown.)

Configuring Device C

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceC-if-range] port link-aggregation group 1
[DeviceC-if-range] quit
```

Configure Bridge-Aggregation 2 as a trunk port, and assign it to VLAN 20.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] port link-type trunk
[DeviceC-Bridge-Aggregation1] port trunk permit vlan 20
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/5 to VLAN 20.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port access vlan 20
[DeviceC-GigabitEthernet1/0/5] quit
```

Configuring Device D

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to VLAN 10, VLAN 30, and VLAN 40, respectively.

```
<DeviceD> system-view
[DeviceD] vlan 10
[DeviceD-vlan10] quit
[DeviceD] interface gigabitethernet1/0/1
[DeviceD-GigabitEthernet1/0/1] port access vlan 10
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] vlan 40
[DeviceD-vlan40] quit
[DeviceD] interface gigabitethernet1/0/3
[DeviceD-GigabitEthernet1/0/3] port access vlan 40
[DeviceD] vlan 30
[DeviceD-vlan30] quit
[DeviceD] interface gigabitethernet1/0/2
[DeviceD-GigabitEthernet1/0/2] port access vlan 30
```

Enable IP multicast routing, and enable PIM-SM on VLAN-interface 10 and VLAN-interface 30.

```
[DeviceD] multicast routing
[DeviceD-mrib] quit
[DeviceD] interface vlan-interface 10
[DeviceD-Vlan-interface10] pim sm
[DeviceD-Vlan-interface10] quit
[DeviceD] vlan 30
[DeviceD-vlan30] quit
[DeviceD] interface vlan-interface 30
[DeviceD-Vlan-interface10] pim sm
[DeviceD-Vlan-interface10] quit
```

Enable IGMPv2 on VLAN-interface 40.

```
[DeviceD] interface vlan-interface 40
[DeviceD-Vlan-interface40] igmp enable
[DeviceD-Vlan-interface40] igmp version 2
[DeviceD-Vlan-interface40] quit
```

Verifying the configuration

Verify that Device B sends and receives keepalive packets correctly.

```
<DeviceB> display drni keepalive
Neighbor keepalive link status (cause): Up
Neighbor is alive for: 176 s 237 ms
Keepalive packet transmission status:
  Sent: Successful
  Received: Successful
Last received keepalive packet information:
  Source IP address: 200.0.0.1
  Time: 2021/12/21 15:12:43
```

```
  Action: Accept

Distributed relay keepalive parameters:
Destination IP address: 200.0.0.1
Source IP address: 200.0.0.2
Keepalive UDP port : 6400
Keepalive VPN name : N/A
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Verify that interfaces used by DRNI operate correctly on Device B.

```
<DeviceB> display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG1
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time(s)
BAGG2         1         UP                   UP          -
```

Verify that the DR interface on Device B operates correctly.

```
<DeviceB> display link-aggregation verbose bridge-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/5(R)          S        32768    32770    40001                  {ACDEF}
  GE1/0/6             S        32768    32770    40001                  {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/5             32768    2        1        0x8000, 84c4-42e5-0300 {ACDEF}
  GE1/0/6             32768    2        1        0x8000, 84c4-42e5-0300 {ACDEF}
```

Verify that the IGMP group information on Device D is correct.

```
<DeviceD> display igmp group
IGMP groups in total: 1
```

```
 Vlan-interface40(40.0.0.2):
  IGMP groups reported in total: 1
   Group address   Last reporter   Uptime      Expires
   225.0.0.1       40.0.0.10       00:02:04    00:01:15
```

Verify that PIM routing entries have been created on Device B.

```
<DeviceB> display pim routing-table
 Total 1 (*, G) entries; 1 (S, G) entries

 (*, 225.0.0.1)
     RP: 2.2.2.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:00:20
     Upstream interface: Register-Tunnel0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface30
             Protocol: pim-sm, UpTime: 00:00:20, Expires: -

 (20.0.0.100, 225.0.0.1)
     RP: 2.2.2.2 (local)
     Protocol: pim-sm, Flag: SPT ACT 2MVPN
     UpTime: 00:00:19
     Upstream interface: Vlan-interface20
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface30
             Protocol: pim-sm, UpTime: 00:00:19, Expires: -
```

Verify that multicast forwarding entries have been created on Device B.

```
<DeviceB> display multicast forwarding-table
Total 1 entries, 1 matched

00001. (20.0.0.100, 225.0.0.1)
     Flags: 0x0
     Uptime: 00:00:55, Timeout in: 00:03:18
     Incoming interface: Vlan-interface20
     List of 1 outgoing interfaces:
       1: Vlan-interface30
     Matched 1293 packets(36204 bytes), Wrong If 0 packets
     Forwarded 1291 packets(36148 bytes)
```

Verify that Device A does not create PIM routing entries or multicast forwarding entries, which indicates that Device B forwards all multicast traffic to the receiver. (Details not shown.)

Configuration files

- Device A:

```
#
 sysname DeviceA
#
ospf 1
 router-id 2.2.2.2
 area 0.0.0.0
#
vlan 1
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
 port drni group 1
#
interface LoopBack0
 ospf 1 area 0.0.0.0
 pim sm
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ospf 1 area 0.0.0.0
 pim sm
 ip address 100.0.0.1 255.255.255.0
#
interface Vlan-interface20
 ospf 1 area 0.0.0.0
 pim sm
 ip address 20.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 20.0.0.10
 vrrp vrid 1 priority 200
#
interface GigabitEthernet1/0/3
 ip address 200.0.0.1 255.255.255.0
#
```

```
interface GigabitEthernet1/0/5
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/6
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port access vlan 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
multicast routing
#
pim
 c-bsr 1.1.1.1
 c-rp 1.1.1.1
#
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 123
 drni keepalive ip destination 200.0.0.2 source 200.0.0.1
 drni mad exclude interface GigabitEthernet1/0/3
#
```

- Device B:

```
#
 sysname DeviceB
#
ospf 1
 router-id 3.3.3.3
 area 0.0.0.0
 area 0.0.0.9
#
vlan 20
#
vlan 30
#
```

```
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
 port drni group 1
#
interface LoopBack0
 ospf 1 area 0.0.0.0
 pim sm
 ip address 2.2.2.2/32
#
interface Vlan-interface20
 ospf 1 area 0.0.0.0
 pim sm
 ip address 20.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 20.0.0.10
 vrrp vrid 1 priority 100
#
interface Vlan-interface30
 ospf 1 area 0.0.0.0
 pim sm
 ip address 30.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 ospf 1 area 0.0.0.0
 ip address 200.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/5
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/6
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port access vlan 30
#
interface GigabitEthernet1/0/1
 port link-type trunk
```

```
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
multicast routing
#
pim
 c-bsr 1.1.1.1
 c-rp 1.1.1.1
#
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 123
 drni keepalive ipv6 destination 200.0.0.1 source 200.0.0.2
 drni mad exclude interface GigabitEthernet1/0/3
#
```

- Device C:

```
#
 sysname DeviceC
#
vlan 1
#
vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/5
 port access vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
```

```
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
```

- Device D:

```
#
 sysname DeviceD
#
ospf 1
 router-id 4.4.4.4
 area 0.0.0.0
#
vlan 10
#
vlan 40
#
vlan 30
#
interface Vlan-interface10
 ospf 1 area 0.0.0.0
 pim sm
 ip address 100.0.0.2 255.255.255.0
#
interface Vlan-interface40
 ospf 1 area 0.0.0.0
 ip address 40.0.0.2 255.255.255.0
 igmp enable
 igmp version 2
#
interface Vlan-interface30
 ospf 1 area 0.0.0.0
 pim sm
 ip address 30.0.0.2 255.255.255.0
#
interface GigabitEthernet1/0/3
 port access vlan 40
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 30
```

```
#
multicast routing
#
```

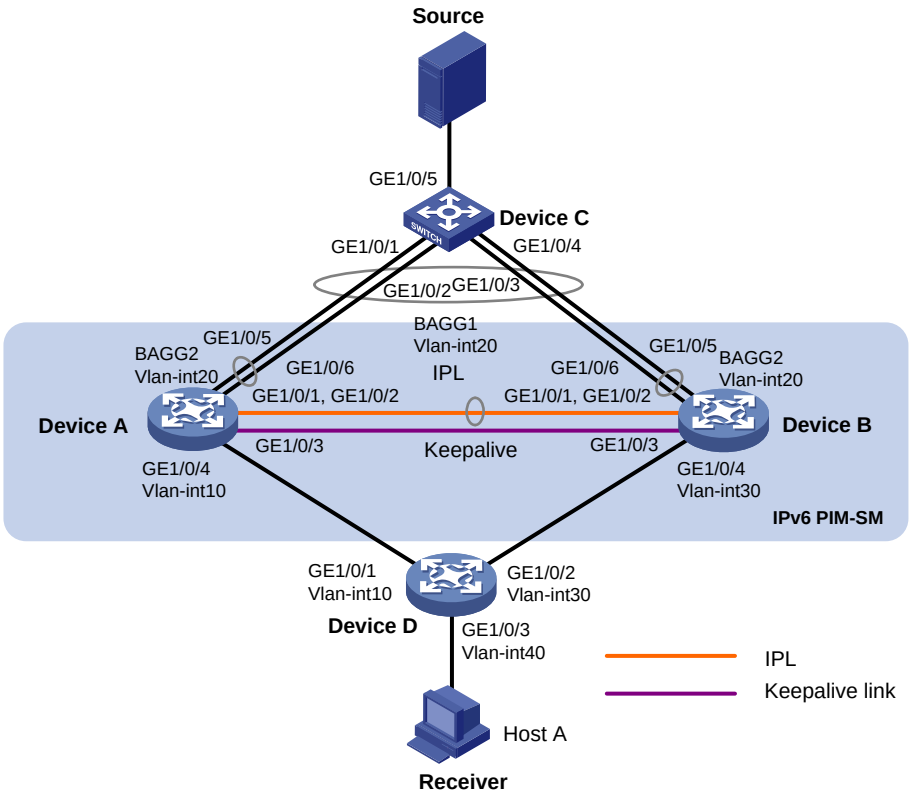
Example: Configuring Layer 3 IPv6 multicast on a DR system attached to multicast sources

Network configuration

As shown in Figure 2:

- OSPFv3 runs on the network.
- VOD streams are sent to receiver hosts in multicast. The receivers of different subnets form stub networks, and a minimum of one receiver host exist on each stub network.
- The entire IPv6 PIM-SM domain contains only one BSR.
- Device C is a Layer 2 device attached to the multicast source. Switch A and Switch B are virtualized into a DR system, which is connected to Switch C through a multichassis aggregate link. VLAN-interface 20 interfaces on the DR system are the gateway for the multicast source.
- Host A is a multicast data receiver attached to Device D.
- The GigabitEthernet 1/0/3 interfaces on Device A and Device B are excluded from the shutdown action by DRNI MAD to set up the keepalive link.
- A VRRP group is configured on VLAN-interface 20 interfaces. In the VRRP group, Device A is the master.
- DR interfaces on Switch A and Switch B permit packets from VLAN 20 to pass through. PIM is enabled on VLAN-interface 20 of Switch A and Switch B.
- IPv6 multicast routing is enabled on Switch A and Switch B.

Figure 2 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-int20	2000::1/80	Device D	Vlan-int10	2003::2/80
	GE1/0/3	2002::1/80		Vlan-int30	2004::2/80
	Vlan-int10	2003::1/80		Vlan-int40	20::1/80
	Loop0	1111::1111/128			
Device B	Vlan-int20	2000::2/80			
	GE1/0/3	2002::2/80			
	Vlan-int30	2004::1/80			
	Loop0	2222::2222/128			

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 or later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 or later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported

Hardware	Software version
S5560X-EI switch series	Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported

Hardware	Software version
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Assigning IPv6 addresses and configuring unicast routing

Assign an IPv6 address and prefix to each interface as shown in Figure 2, and configure OSPFv3 on the switches in the IPv6 PIM-SM domain. (Details not shown.)

Configuring Device A

Configure the DR system settings.

```
<DeviceA> system-view
[DeviceA] drni system-mac 1-1-1
[DeviceA] drni system-number 1
[DeviceA] drni system-priority 123
```

Configure DR keepalive packet parameters.

```
[DeviceA] drni keepalive ipv6 destination 2002::2 source 2002::1
```

Exclude the interface used for DR keepalive detection (GigabitEthernet 1/0/3) from the shutdown action by DRNI MAD.

```
[DeviceA] drni mad exclude interface gigabitethernet 1/0/3
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/2] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/5 and GigabitEthernet 1/0/6 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/5] quit
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/6] quit
```

Configure Bridge-Aggregation 1 as a trunk port, assign it to all VLANs, and specify it as the IPP.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
[DeviceA-Bridge-Aggregation1] port trunk permit vlan all
[DeviceA-Bridge-Aggregation1] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation1] quit
```

Configure Bridge-Aggregation 2 as a trunk port, assign it to VLAN 20, and assign it to a DR group.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] port link-type trunk
[DeviceA-Bridge-Aggregation2] port trunk permit vlan 20
[DeviceA-Bridge-Aggregation2] port drni group 1
[DeviceA-Bridge-Aggregation2] quit
```

Configure VRRP group 1 on VLAN-interface 20, and set the priority of Device A to 200 for it to become the master in the VRRP group.

```
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
[DeviceA-Vlan-interface20] vrrp ipv6 vrid 1 virtual-ip 2000::10
[DeviceA-Vlan-interface20] vrrp ipv6 vrid 1 priority 200
[DeviceA-Vlan-interface20] quit
```

Enable IPv6 multicast routing, enable MLD and IPv6 PIM on VLAN-interface 10, and enable IPv6 PIM-SM on other interfaces as required.

```
[DeviceA] ipv6 multicast routing
```

```
[DeviceA-mrib6] quit
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] mld enable
[DeviceA-Vlan-interface10] ipv6 pim sm
[DeviceA-Vlan-interface10] quit
[DeviceA] interface vlan-interface 20
[DeviceA-Vlan-interface20] ipv6 pim sm
[DeviceA-Vlan-interface20] quit
[DeviceA] interface loopback 0
[DeviceA-LoopBack0] ipv6 pim sm
[DeviceA-LoopBack0] quit
```

Specify the IPv6 address of Loopback 0 as a C-RP and a C-BSR.

```
[DeviceA] ipv6 pim
[DeviceA-pim6] c-rp 1111::1111
[DeviceA-pim6] c-bsr 1111::1111
[DeviceA-pim6] quit
```

Configuring Device B

Configure Device B in the same way you configure Device A. (Details not shown.)

Configuring Device C

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceC-if-range] port link-aggregation group 1
[DeviceC-if-range] quit
```

Configure Bridge-Aggregation 2 as a trunk port, and assign it to VLAN 20.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] port link-type trunk
[DeviceC-Bridge-Aggregation1] port trunk permit vlan 20
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/5 to VLAN 20.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port access vlan 20
[DeviceC-GigabitEthernet1/0/5] quit
```

Configuring Device D

Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to VLAN 10, VLAN 30, and VLAN 40, respectively.

```
<DeviceD> system-view
[DeviceD] vlan 10
```

```
[DeviceD-vlan10] quit
[DeviceD] interface gigabitethernet1/0/1
[DeviceD-GigabitEthernet1/0/1] port access vlan 10
[DeviceD-GigabitEthernet1/0/1] quit
[DeviceD] vlan 40
[DeviceD-vlan40] quit
[DeviceD] interface gigabitethernet1/0/3
[DeviceD-GigabitEthernet1/0/3] port access vlan 40
[DeviceD] vlan 30
[DeviceD-vlan30] quit
[DeviceD] interface gigabitethernet1/0/2
[DeviceD-GigabitEthernet1/0/2] port access vlan 30
```

Enable IPv6 multicast routing, and enable IPv6 PIM-SM on VLAN-interface 10 and VLAN-interface 30.

```
[DeviceD] ipv6 multicast routing
[DeviceD-mrib6] quit
[DeviceD] interface vlan-interface 10
[DeviceD-Vlan-interface10] ipv6 pim sm
[DeviceD-Vlan-interface10] quit
[DeviceD] vlan 30
[DeviceD-vlan30] quit
[DeviceD] interface vlan-interface 30
[DeviceD-Vlan-interface30] ipv6 pim sm
[DeviceD-Vlan-interface30] quit
```

Enable MLDv2 on VLAN-interface 40.

```
[DeviceD] interface vlan-interface 40
[DeviceD-Vlan-interface40] mld enable
[DeviceD-Vlan-interface40] mld version 2
[DeviceD-Vlan-interface40] quit
```

Verifying the configuration

Verify that Device B sends and receives keepalive packets correctly.

```
<DeviceB> display drni keepalive
Neighbor keepalive link status (cause): Up
Neighbor is alive for: 2128 s 421 ms
Keepalive packet transmission status:
  Sent: Successful
  Received: Successful
Last received keepalive packet information:
  Source IP address: 2002::1
  Time: 2021/12/21 15:45:15
  Action: Accept

Distributed relay keepalive parameters:
Destination IP address: 2002::1
Source IP address: 2002::2
Keepalive UDP port : 6400
```

```
Keepalive VPN name : N/A
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Verify that interfaces used by DRNI operate correctly on Device B.

```
<DeviceB> display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG1
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time(s)
BAGG2         1         UP                   UP          -
```

Verify that the DR interface on Device B operates correctly.

```
<DeviceB> display link-aggregation verbose bridge-aggregation 2

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation2
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x7b, 0001-0001-0001
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/5(R)          S        32768    32770    40001                  {ACDEF}
  GE1/0/6             S        32768    32770    40001                  {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/5             32768    2        1        0x8000, 84c4-42e5-0300 {ACDEF}
  GE1/0/6             32768    2        1        0x8000, 84c4-42e5-0300 {ACDEF}
```

Verify that the MLD group information on Device D is correct.

```
<DeviceD> display mld group
MLD groups in total: 1
 Vlan-interface40(FE80::200:FCFF:FE00:3472):
  MLD groups reported in total: 1
   Group address: FF08::2
    Last reporter: FE80::1
    Uptime: 01:56:46
```

```
    Expires: 00:02:43
```

Verify that IPv6 PIM routing entries have been created on Device B.

```
<DeviceB> display ipv6 pim routing-table
 Total 1 (*, G) entries; 1 (S, G) entries
 (*, FF08::2)
     RP: 2222::2222(local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:17:51
     Upstream interface: Register-Tunnel0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface30
             Protocol: pim-sm, UpTime: 00:17:51, Expires: 00:02:39
 (2000::111, FF08::2)
     RP: 2222::2222(local)
     Protocol: pim-sm, Flag: SPT LOC ACT 2MVPN
     UpTime: 00:17:54
     Upstream interface: Vlan-interface20
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface information:
     Total number of downstream interfaces: 1
         1: Vlan-interface30
             Protocol: pim-sm, UpTime: 00:17:54, Expires: 00:02:36
```

Verify that IPv6 multicast forwarding entries have been created on Device B.

```
<DeviceB> display ipv6 multicast forwarding-table
Total 1 entries, 1 matched

00001. (2000::111, FF08::2)
     Flags: 0x0
     Uptime: 00:08:27, Timeout in: 00:03:27
     Incoming interface: Vlan-interface20
     List of 1 outgoing interfaces:
       1: Vlan-interface30
     Matched 5 packets(71681 bytes), Wrong If 0 packets
     Forwarded 5 packets(71681 bytes)
```

Verify that Device A does not create IPv6 PIM routing entries or multicast forwarding entries, which indicates that Device B forwards all multicast traffic to the receiver. (Details not shown.)

Configuration files

- Device A:

```
#
 sysname DeviceA
#
```

```
ospfv3 1
 router-id 2.2.2.2
 area 0.0.0.0
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
 port drni group 1
#
interface LoopBack0
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 1111::1111/128
#
interface Vlan-interface10
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2003::1/80
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2000::1/80
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 2000::10
 vrrp ipv6 vrid 1 priority 200
#
interface GigabitEthernet1/0/3
 ipv6 address 2002::1/80
#
interface GigabitEthernet1/0/5
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/6
 port link-type trunk
```

```
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port access vlan 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
ipv6 multicast routing
#
ipv6 pim
 c-bsr 1111::1111
 c-rp 1111::1111
#
 drni system-mac 0001-0001-0001
 drni system-number 1
 drni system-priority 123
 drni keepalive ipv6 destination 2002::2 source 2002::1
 drni mad exclude interface GigabitEthernet1/0/3
#
```

- Device B:

```
#
 sysname DeviceB
#
ospfv3 1
 router-id 3.3.3.3
 area 0.0.0.0
#
vlan 20
#
vlan 30
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port drni intra-portal-port 1
#
interface Bridge-Aggregation2
 port link-type trunk
```

```
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
 port drni group 1
#
interface LoopBack0
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2222::2222/128
#
interface Vlan-interface20
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2000::2/80
 vrrp ipv6 vrid 1 virtual-ip FE80::10 link-local
 vrrp ipv6 vrid 1 virtual-ip 2000::10
 vrrp ipv6 vrid 1 priority 100

#
interface Vlan-interface30
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2004::1/80
#
interface GigabitEthernet1/0/3
 ospfv3 1 area 0.0.0.0
 ipv6 address 2002::2/80
#
interface GigabitEthernet1/0/5
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/6
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/4
 port access vlan 30
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
```

```
 port link-aggregation group 1
#
ipv6 multicast routing
#
ipv6 pim
 c-bsr 2222::2222
 c-rp 2222::2222
#
 drni system-mac 0001-0001-0001
 drni system-number 2
 drni system-priority 123
 drni keepalive ipv6 destination 2002::1 source 2002::2
 drni mad exclude interface GigabitEthernet1/0/3
#
```

- Device C:

```
#
 sysname DeviceC
#
vlan 20
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 20
 link-aggregation mode dynamic
#
interface LoopBack1
 ipv6 address FE80::2 link-local
#
interface GigabitEthernet1/0/5
 port access vlan 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-type trunk
```

```
 port trunk permit vlan 1 20
 port link-aggregation group 1
#
```

- Device D:

```
#
 sysname DeviceD
#
ospfv3 1
 router-id 4.4.4.4
 area 0.0.0.0
#
vlan 10
#
vlan 40
#
vlan 30
#
interface Vlan-interface10
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2003::2/80
#
interface Vlan-interface40
 ospfv3 1 area 0.0.0.0
 ipv6 address 20::1/80
 mld enable
 mld version 2
#
interface Vlan-interface30
 ospfv3 1 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2004::2/80
#
interface GigabitEthernet1/0/3
 port access vlan 40
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 30
#
ipv6 multicast routing
#
pim
#
```

Contents

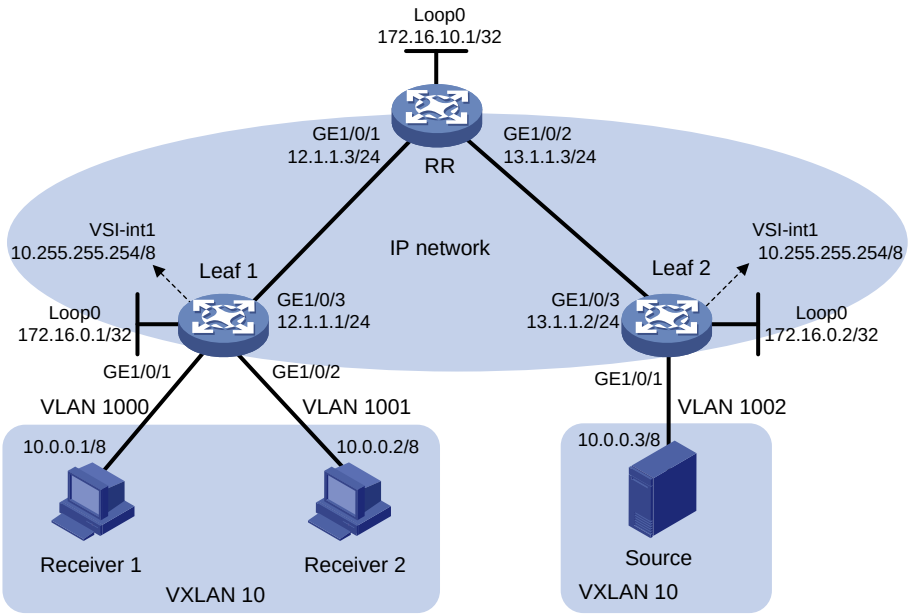
Example: Configuring Layer 2 EVPN multicast

Network configuration

As shown in Figure 1, configure Layer 2 EVPN multicast as follows:

- Configure Leaf 1 and Leaf 2 as distributed EVPN gateways. Assign the multicast receivers attached to Leaf 1 and the multicast source attached to Leaf 2 to VXLAN 10.
- Configure Leaf 1, Leaf 2, and the RR to set up BGP EVPN peer relationships in AS 65000 of the overlay network. Configure the RR to reflect BGP EVPN routes between Leaf 1 and Leaf 2.
- Configure OSPF on Leaf 1, Leaf 2, and the RR for them to have Layer 3 connectivity on the underlay network.

Figure 1 Network diagram



Analysis

To enable Layer 2 multicast forwarding in the EVPN network, perform the following tasks:

- Enable IGMP snooping on the leaf devices for them to snoop the IGMP membership reports sent by the multicast receivers.
- For the leaf devices to create Layer 2 multicast forwarding entries, configure the leaf devices to advertise multicast group join requests through selective multicast Ethernet tag (SMET) routes.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch	Not supported

Restrictions and guidelines

IGMP snooping restrictions and guideline

IGMP snooping configuration in a VSI takes effect only on the member ports in the VSI.

In an EVPN VXLAN network, the IGMP snooping querier in a VSI does not include VLAN tags in IGMP general queries. As a best practice, do not enable the IGMP snooping querier in a VSI if the VSI uses the Ethernet access mode.

Distributed EVPN gateway restrictions and guideline

When you configure VSI interfaces on distributed EVPN gateways, follow these restrictions and guidelines:

- Do not assign reserved MAC addresses to VSI interfaces.
- You must assign the same MAC address to the VSI interfaces with L3 VXLAN IDs associated
- If you use the **mac-address** command to modify the MAC address of a L3 VXLAN ID associated VSI interface on a DR system, also modify the MAC address of the other L3 VXLAN ID associated VSI interfaces. These VSI interfaces must use the same MAC address.
- If a distributed EVPN gateway is connected to an IPv6 site, make sure the VSI interfaces with L3 VXLAN IDs associated use the same link-local address.
- On different distributed EVPN gateways, the VSI interface of a VXLAN must use the same IP address and MAC address to provide services.
- The L3 VXLAN ID of a VSI interface cannot be the same as the VXLAN ID specified by using the **mapping vni** command.
- As a best practice, do not use ARP flood suppression and local proxy ARP or ND flood suppression and local ND proxy together on distributed EVPN gateways. If both ARP flood suppression and local proxy ARP are enabled on a distributed EVPN gateway, only local proxy ARP takes effect. If both ND flood suppression and local ND proxy are enabled on a distributed EVPN gateway, only local ND proxy takes effect.

Procedures

Configuring Leaf 1

Setting the system operating mode to VXLAN

Set system operating mode to VXLAN, save the running configuration, and reboot the device.

```
<Sysname> system-view
[Sysname] switch-mode 1
Reboot device to make the configuration take effect.
[Sysname] quit
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Assigning IP addresses and configuring unicast routing

Assign IP addresses to loopback interfaces and GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] sysname Leaf1
[Leaf1] interface loopback 0
[Leaf1-LoopBack0] ip address 172.16.0.1 255.255.255.255
[Leaf1-LoopBack0] quit
```

```
[Leaf1] interface gigabitethernet 1/0/3
[Leaf1-GigabitEthernet1/0/3] port link-mode route
[Leaf1-GigabitEthernet1/0/3] ip address 12.1.1.1 24
[Leaf1-GigabitEthernet1/0/3] quit
```

Configure OSPF for the devices to communicate at Layer 3 over the underlay network.

```
[Leaf1] router id 172.16.0.1
[Leaf1] ospf
[Leaf1-ospf-1] area 0
[Leaf1-ospf-1-area-0.0.0.0] network 172.16.0.1 0.0.0.0
[Leaf1-ospf-1-area-0.0.0.0] network 12.1.1.1 0.0.0.255
[Leaf1-ospf-1-area-0.0.0.0] quit
[Leaf1-ospf-1] quit
```

Configuring a VPN instance

Create VPN instance **vpn1** and configure an RD and route targets for it.

```
[Leaf1] ip vpn-instance vpn1
[Leaf1-vpn-instance-vpn1] route-distinguisher 1:1
[Leaf1-vpn-instance-vpn1] address-family ipv4
[Leaf1-vpn-ipv4-vpn1] vpn-target 2:2 import-extcommunity
[Leaf1-vpn-ipv4-vpn1] vpn-target 2:2 export-extcommunity
[Leaf1-vpn-ipv4-vpn1] quit
[Leaf1-vpn-instance-vpn1] address-family evpn
[Leaf1-vpn-evpn-vpn1] vpn-target 1:1 import-extcommunity
[Leaf1-vpn-evpn-vpn1] vpn-target 1:1 export-extcommunity
[Leaf1-vpn-evpn-vpn1] quit
[Leaf1-vpn-instance-vpn1] quit
```

Configuring a VSI interface

Enable L2VPN.

```
[Leaf1] l2vpn enable
```

Configure VSI interface 1.

```
[Leaf1] interface vsi-interface 1
[Leaf1-Vsi-interface1] ip binding vpn-instance vpn1
[Leaf1-Vsi-interface1] ip address 10.255.255.254 255.0.0.0
[Leaf1-Vsi-interface1] mac-address 0000-0001-0001
[Leaf1-Vsi-interface1] distributed-gateway local
[Leaf1-Vsi-interface1] quit
```

Configuring an EVPN instance

Disable remote MAC address learning and remote ARP learning.

```
[Leaf1] vxlan tunnel mac-learning disable
[Leaf1] vxlan tunnel arp-learning disable
```

Create VXLAN 10 on VSI **vsi1**, and specify VSI interface 1 as the gateway for the VXLAN.

```
[Leaf1] vsi vsi1
[Leaf1-vsi-vsi1] gateway vsi-interface 1
[Leaf1-vsi-vsi1] statistics enable
[Leaf1-vsi-vsi1] arp suppression enable
[Leaf1-vsi-vsi1] vxlan 10
[Leaf1-vsi-vsi1-vxlan-10] quit
```

Configure an EVPN instance using VXLAN encapsulation, and configure an RD and route targets for it.

```
[Leaf1-vsi-vsi1] evpn encapsulation vxlan
[Leaf1-vsi-vsi1-evpn-vxlan] route-distinguisher auto
[Leaf1-vsi-vsi1-evpn-vxlan] vpn-target auto export-extcommunity
[Leaf1-vsi-vsi1-evpn-vxlan] vpn-target auto import-extcommunity
[Leaf1-vsi-vsi1-evpn-vxlan] quit
[Leaf1-vsi-vsi1] quit
```

Assigning L3 VXLAN IDs

Assign a L3 VXLAN ID to VSI interface 2.

```
[Leaf1] interface vsi-interface 2
[Leaf1-Vsi-interface2] ip binding vpn-instance vpn1
[Leaf1-Vsi-interface2] l3-vni 10000
[Leaf1-Vsi-interface2] quit
```

Configuring BGP EVPN route advertisement

Configure Leaf 1 to establish a BGP EVPN peer relationship with the RR.

```
[Leaf1] bgp 65000
[Leaf1-bgp-default] peer 172.16.10.1 as-number 65000
[Leaf1-bgp-default] peer 172.16.10.1 connect-interface loopback 0
[Leaf1-bgp-default] peer 172.16.10.1 password simple overlay
[Leaf1-bgp-default] address-family l2vpn evpn
[Leaf1-bgp-default-evpn] peer 172.16.10.1 enable
[Leaf1-bgp-default-evpn] quit
[Leaf1-bgp-default] quit
```

Mapping ACs to the VSI

On GigabitEthernet 1/0/1, create Ethernet service instance 1 and map it to VSI **vsi1**.

```
[Leaf1] interface gigabitethernet 1/0/1
[Leaf1-GigabitEthernet1/0/1] port link-mode bridge
[Leaf1-GigabitEthernet1/0/1] port link-type trunk
[Leaf1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Leaf1-GigabitEthernet1/0/1] port trunk permit vlan 1000
[Leaf1-GigabitEthernet1/0/1] service-instance 1
[Leaf1-GigabitEthernet1/0/1-srv1] encapsulation s-vid 1000
[Leaf1-GigabitEthernet1/0/1-srv1] statistics enable
[Leaf1-GigabitEthernet1/0/1-srv1] xconnect vsi vsi1
[Leaf1-GigabitEthernet1/0/1-srv1] quit
[Leaf1-GigabitEthernet1/0/1] quit
```

On GigabitEthernet 1/0/2, create Ethernet service instance 1 and map it to VSI **vsi1**.

```
[Leaf1] interface gigabitethernet 1/0/2
[Leaf1-GigabitEthernet1/0/2] port link-mode bridge
[Leaf1-GigabitEthernet1/0/2] port link-type trunk
[Leaf1-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Leaf1-GigabitEthernet1/0/2] port trunk permit vlan 1001
[Leaf1-GigabitEthernet1/0/2] service-instance 1
[Leaf1-GigabitEthernet1/0/2-srv1] encapsulation s-vid 1001
[Leaf1-GigabitEthernet1/0/2-srv1] statistics enable
[Leaf1-GigabitEthernet1/0/2-srv1] xconnect vsi vsi1
```

```
[Leaf1-GigabitEthernet1/0/2-srv1] quit
[Leaf1-GigabitEthernet1/0/2] quit
```

Configuring IGMP snooping

Enable IGMP snooping globally.

```
[Leaf1] igmp-snooping
[Leaf1-igmp-snooping] global-enable
[Leaf1-igmp-snooping] quit
```

Configure IGMP snooping for VSI **vsi1**.

```
[Leaf1] vsi vsi1
[Leaf1-vsi-vsi1] igmp-snooping enable
[Leaf1-vsi-vsi1] igmp-snooping drop-unknown
[Leaf1-vsi-vsi1] igmp-snooping proxy enable
```

Configure Leaf 2 as an IGMP querier.

```
[Leaf1-vsi-vsi1] igmp-snooping querier
[Leaf1-vsi-vsi1] quit
```

Configuring Leaf 2

Setting the system operating mode to VXLAN

Set system operating mode to VXLAN, save the running configuration, and reboot the device.

```
<Sysname> system-view
[Sysname] switch-mode 1
Reboot device to make the configuration take effect.
[Sysname] quit
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Assigning IP addresses and configuring unicast routing

Assign IP addresses to loopback interfaces and GigabitEthernet 1/0/3.

```
<Sysname> system-view
[Sysname] sysname Leaf2
[Leaf2] interface loopback 0
[Leaf2-LoopBack0] ip address 172.16.0.2 255.255.255.255
[Leaf2-LoopBack0] quit
[Leaf2] interface gigabitethernet 1/0/3
[Leaf2-GigabitEthernet1/0/3] port link-mode route
[Leaf2-GigabitEthernet1/0/3] ip address 13.1.1.2 24
[Leaf2-GigabitEthernet1/0/3] quit
```

Configure OSPF for the devices to communicate at Layer 3 over the underlay network.

```
[Leaf2] router id 172.16.0.2
[Leaf2] ospf
[Leaf2-ospf-1] area 0
[Leaf2-ospf-1-area-0.0.0.0] network 172.16.0.2 0.0.0.0
```

```
[Leaf2-ospf-1-area-0.0.0.0] network 13.1.1.2 0.0.0.255
[Leaf2-ospf-1-area-0.0.0.0] quit
[Leaf2-ospf-1] quit
```

Configuring a VPN instance

Create VPN instance **vpn1** and configure an RD and route targets for it.

```
[Leaf2] ip vpn-instance vpn1
[Leaf2-vpn-instance-vpn1] route-distinguisher 1:1
[Leaf2-vpn-instance-vpn1] address-family ipv4
[Leaf2-vpn-ipv4-vpn1] vpn-target 2:2 import-extcommunity
[Leaf2-vpn-ipv4-vpn1] vpn-target 2:2 export-extcommunity
[Leaf2-vpn-ipv4-vpn1] quit
[Leaf2-vpn-instance-vpn1] address-family evpn
[Leaf2-vpn-evpn-vpn1] vpn-target 1:1 import-extcommunity
[Leaf2-vpn-evpn-vpn1] vpn-target 1:1 export-extcommunity
[Leaf2-vpn-evpn-vpn1] quit
[Leaf2-vpn-instance-vpn1] quit
```

Configuring a VSI interface

Enable L2VPN.

```
[Leaf2] l2vpn enable
```

Configure VSI interface 1.

```
[Leaf2] interface vsi-interface 1
[Leaf2-Vsi-interface1] ip binding vpn-instance vpn1
[Leaf2-Vsi-interface1] ip address 10.255.255.254 255.0.0.0
[Leaf2-Vsi-interface1] mac-address 0000-0001-0001
[Leaf2-Vsi-interface1] distributed-gateway local
[Leaf2-Vsi-interface1] quit
```

Configuring an EVPN instance

Disable remote MAC address learning and remote ARP learning.

```
[Leaf2] vxlan tunnel mac-learning disable
[Leaf2] vxlan tunnel arp-learning disable
```

Create VXLAN 10 on VSI **vsi1**, and specify VSI interface 1 as the gateway for the VXLAN.

```
[Leaf2] vsi vsi1
[Leaf2-vsi-vsi1] gateway vsi-interface 1
[Leaf2-vsi-vsi1] statistics enable
[Leaf2-vsi-vsi1] arp suppression enable
[Leaf2-vsi-vsi1] vxlan 10
[Leaf2-vsi-vsi1-vxlan-10] quit
```

Configure an EVPN instance using VXLAN encapsulation, and configure an RD and route targets for it.

```
[Leaf2-vsi-vsi1] evpn encapsulation vxlan
[Leaf2-vsi-vsi1-evpn-vxlan] route-distinguisher auto
[Leaf2-vsi-vsi1-evpn-vxlan] vpn-target auto export-extcommunity
[Leaf2-vsi-vsi1-evpn-vxlan] vpn-target auto import-extcommunity
[Leaf2-vsi-vsi1-evpn-vxlan] quit
[Leaf2-vsi-vsi1] quit
```

Assigning L3 VXLAN IDs

Assign a L3 VXLAN ID to VSI interface 2.

```
[Leaf2] interface vsi-interface 10000
[Leaf2-Vsi-interface10000] ip binding vpn-instance vpn1
[Leaf2-Vsi-interface10000] l3-vni 10000
[Leaf2-Vsi-interface10000] quit
```

Configuring BGP EVPN route advertisement

Configure Leaf 2 to establish a BGP EVPN peer relationship with the RR.

```
[Leaf2] bgp 65000
[Leaf2-bgp-default] peer 172.16.10.1 as-number 65000
[Leaf2-bgp-default] peer 172.16.10.1 connect-interface loopback 0
[Leaf2-bgp-default] peer 172.16.10.1 password simple overlay
[Leaf2-bgp-default] address-family l2vpn evpn
[Leaf2-bgp-default-evpn] peer 172.16.10.1 enable
[Leaf2-bgp-default-evpn] quit
[Leaf2-bgp-default] quit
```

Mapping ACs to the VSI

On GigabitEthernet 1/0/1, create Ethernet service instance 1 and map it to VSI **vsi1**.

```
[Leaf2] interface gigabitethernet 1/0/1
[Leaf2-GigabitEthernet1/0/1] port link-mode bridge
[Leaf2-GigabitEthernet1/0/1] port link-type trunk
[Leaf2-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Leaf2-GigabitEthernet1/0/1] port trunk permit vlan 1002
[Leaf2-GigabitEthernet1/0/1] storm-constrain control shutdown
[Leaf2-GigabitEthernet1/0/1] service-instance 1
[Leaf2-GigabitEthernet1/0/1-srv1] encapsulation s-vid 1002
[Leaf2-GigabitEthernet1/0/1-srv1] statistics enable
[Leaf2-GigabitEthernet1/0/1-srv1] xconnect vsi vsi1
[Leaf2-GigabitEthernet1/0/1-srv1] quit
[Leaf2-GigabitEthernet1/0/1] quit
```

Configuring IGMP snooping

Enable IGMP snooping globally.

```
[Leaf1] igmp-snooping
[Leaf1-igmp-snooping] global-enable
[Leaf1-igmp-snooping] quit
```

Configure IGMP snooping for VSI **vsi1**.

```
[Leaf2] vsi vsi1
[Leaf2-vsi-vsi1] igmp-snooping enable
[Leaf2-vsi-vsi1] igmp-snooping drop-unknown
[Leaf2-vsi-vsi1] igmp-snooping proxy enable
```

Configure Leaf 2 as an IGMP querier.

```
[Leaf2-vsi-vsi1] igmp-snooping querier
[Leaf2-vsi-vsi1] quit
```

Configuring the RR

Setting the system operating mode to VXLAN

Set system operating mode to VXLAN, save the running configuration, and reboot the device.

```
<Sysname> system-view
[Sysname] switch-mode 1
Reboot device to make the configuration take effect.
[Sysname] quit
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait..
.......DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
This command will reboot the device. Continue? [Y/N]:y
```

Assigning IP addresses and configuring unicast routing

Assign IP addresses to loopback interfaces, GigabitEthernet 1/0/1, and GigabitEthernet 1/0/2.

```
<Sysname> system-view
[Sysname] sysname RR
[RR] interface loopback 0
[RR-LoopBack0] ip address 172.16.10.1 255.255.255.255
[RR-LoopBack0] quit
[RR] interface gigabitethernet 1/0/1
[RR-GigabitEthernet1/0/1] port link-mode route
[RR-GigabitEthernet1/0/1] ip address 12.1.1.3 24
[RR-GigabitEthernet1/0/1] quit
[RR] interface gigabitethernet 1/0/2
[RR-GigabitEthernet1/0/2] port link-mode route
[RR-GigabitEthernet1/0/2] ip address 13.1.1.3 24
[RR-GigabitEthernet1/0/2] quit
```

Configure OSPF for the devices to communicate at Layer 3 over the underlay network.

```
[RR] router id 172.16.10.1
[RR] ospf
[RR-ospf-1] area 0
[RR-ospf-1-area-0.0.0.0] network 172.16.10.1 0.0.0.0
[RR-ospf-1-area-0.0.0.0] network 12.1.1.3 0.0.0.255
[RR-ospf-1-area-0.0.0.0] network 13.1.1.3 0.0.0.255
[RR-ospf-1-area-0.0.0.0] quit
[RR-ospf-1] quit
```

Configuring BGP EVPN route advertisement

Assign Leaf 1 and Leaf 2 to IBGP peer group **leaf**.

```
[RR] bgp 65000
[RR-bgp-default] group leaf internal
[RR-bgp-default] peer leaf connect-interface loopback 0
[RR-bgp-default] peer leaf password simple overlay
[RR-bgp-default] peer 172.16.0.1 group leaf
[RR-bgp-default] peer 172.16.0.2 group leaf
```

Configure the device as an RR, configure it to establish BGP EVPN peer relationships with IBGP peer group **leaf**, and disable route target filtering of received BGP EVPN routes.

```
[RR-bgp-default] address-family l2vpn evpn
[RR-bgp-default-evpn] undo policy vpn-target
[RR-bgp-default-evpn] peer leaf enable
[RR-bgp-default-evpn] peer leaf reflect-client
[RR-bgp-default-evpn] quit
[RR-bgp-default] quit
```

Verifying the configuration

Verifying routing information

Verify that the leaf devices and the RR have learned one another's OSPF routes and can communicate at Layer 3 over the underlay network.

```
[Leaf1] display ip routing-table

Destinations : 16       Routes : 16

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
12.1.1.0/24        Direct  0   0           12.1.1.1        GE1/0/3
12.1.1.0/32        Direct  0   0           12.1.1.1        GE1/0/3
12.1.1.1/32        Direct  0   0           127.0.0.1       InLoop0
12.1.1.255/32      Direct  0   0           12.1.1.1        GE1/0/3
13.1.1.0/24        O_INTRA 10  2           12.1.1.3        GE1/0/3
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
172.16.0.1/32      Direct  0   0           127.0.0.1       InLoop0
172.16.0.2/32      O_INTRA 10  2           12.1.1.3        GE1/0/3
172.16.10.1/32     O_INTRA 10  1           12.1.1.3        GE1/0/3
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Verify that the leaf devices and the RR have established BGP EVPN peer relationships with one another.

```
[Leaf1] display bgp peer l2vpn evpn

 BGP local router ID: 172.16.0.1
 Local AS number: 65000
 Total number of peers: 1                 Peers in established state: 1

  * - Dynamically created peer
  ^ - Peer created through link-local address
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
```

```
  172.16.10.1          65000       24       27    0       4 00:14:59 Established
```

Verifying VSI configuration

Verify that VXLAN tunnels and ACs are correctly mapped to VSI **vsi1**.

```
[Leaf1] display l2vpn vsi verbose
VSI Name: Auto_L3VNI10000_2
  VSI Index               : 1
  VSI State               : Down
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 2
  VXLAN ID                : 10000

VSI Name: vsi1
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Enabled
  Input Statistics        :
    Octets   :0
    Packets  :0
    Errors   :0
    Discards :0
  Output Statistics       :
    Octets   :0
    Packets  :0
    Errors   :0
    Discards :0
  Gateway Interface       : VSI-interface 1
```

```
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name           Link ID    State    Type        Flood proxy
    Tunnel0               0x5000000  UP       Auto        Disabled
  ACs:
    AC                                  Link ID    State       Type
    GE1/0/1 srv1                        0          Up          Manual
    GE1/0/2 srv1                        1          Up          Manual
```

Verifying IGMP snooping and SMET routes

Verify that IGMP snooping is enabled on a per-VSI basis on the leaf devices.

```
[Leaf1] display igmp-snooping vsi vsi1
IGMP snooping information: VSI vsi1
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP:10.255.255.254, Expires: 00:01:39)
 Querier-election: Disabled
 Query-interval: 125s
 General-query source IP: 10.255.255.254
 Special-query source IP: 10.255.255.254
 Report source IP: 10.255.255.254
 Leave source IP: 10.255.255.254
 Proxy: Enabled
 IPP: -(Link ID: 0xffff)
```

Verify that Leaf 1 has a dynamic IGMP snooping group entry for multicast group (0.0.0.0, 225.0.0.1).

```
[Leaf1] display igmp-snooping group
Total 1 entries.

VSI vsi1: Total 1 entries.
  (0.0.0.0, 225.0.0.1)
    Host ports (1 in total):
      GE1/0/1 (Link ID 0)                         (00:03:42)
```

Verify that Leaf 1 has created an SMET route.

```
[Leaf1] display evpn route smet
VSI name: vsi1
  Source address :
  Group address  : 225.0.0.1
  Local version  : v2
  ACs   :
    AC                                Link ID    Flags
    GE1/0/1 srv1                      0          Local
```

Verify that Leaf 2 has received the SMET route created by Leaf 1.

```
[Leaf2] display evpn route smet
VSI name: vsi1
  Source address :
  Group address  : 225.0.0.1
  Local version  : -
  Peers :
    Nexthop          Tunnel name     Link ID    Remote version
    172.16.0.1       Tunnel0         0x5000000  v2
```

Verify that Leaf 1 has a dynamic IGMP snooping group entry for multicast group (0.0.0.0, 225.0.0.1).

```
[Leaf2] display igmp-snooping evpn-group
Total 1 entries.

VSI vsi1: Total 1 entries.
  (0.0.0.0, 225.0.0.1)
    Host ports (1 in total):
      Tun0 (VXLAN ID 10)
```

Configuration files

- Leaf 1:

```
#
 sysname Leaf1
#
ip vpn-instance vpn1
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
 router id 172.16.0.1
#
ospf 1
 area 0.0.0.0
  network 12.1.1.0 0.0.0.255
  network 172.16.0.1 0.0.0.0
#
igmp-snooping
 global-enable
#
```

```
 l2vpn enable
 vxlan tunnel arp-learning disable
#
vsi vsi1
 gateway vsi-interface 1
 statistics enable
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping querier
 igmp-snooping proxy enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1000
#
 service-instance 1
  encapsulation s-vid 1000
  statistics enable
  xconnect vsi vsi1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1001
#
 service-instance 1
  encapsulation s-vid 1001
  statistics enable
  xconnect vsi vsi1
#
interface LoopBack0
 ip address 172.16.0.1 255.255.255.255
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 12.1.1.1 255.255.255.0
#
interface Vsi-interface1
```

```
 ip binding vpn-instance vpn1
 ip address 10.255.255.254 255.0.0.0
 mac-address 0000-0001-0001
 distributed-gateway local
#
interface Vsi-interface2
 ip binding vpn-instance vpn1
 l3-vni 10000
#
bgp 65000
 peer 172.16.10.1 as-number 65000
 peer 172.16.10.1 connect-interface LoopBack0
 peer 172.16.10.1 password cipher $c$3$cLxsbhBfj0xOTCgIQD1N6k3oJBamRAhZ5d8=
 #
 address-family l2vpn evpn
  peer 172.16.10.1 enable
#
return
```

- Leaf 2:

```
#
 sysname Leaf2
#
ip vpn-instance vpn1
 route-distinguisher 1:1
 #
 address-family ipv4
  vpn-target 2:2 import-extcommunity
  vpn-target 2:2 export-extcommunity
 #
 address-family evpn
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
#
 vxlan tunnel mac-learning disable
#
 router id 172.16.0.2
#
ospf 1
 area 0.0.0.0
  network 13.1.1.0 0.0.0.255
  network 172.16.0.2 0.0.0.0
#
igmp-snooping
 global-enable
#
 l2vpn enable
 vxlan tunnel arp-learning disable
#
```

```
vsi vsi1
 gateway vsi-interface 1
 statistics enable
 arp suppression enable
 vxlan 10
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping querier
 igmp-snooping proxy enable
#
interface LoopBack0
 ip address 172.16.0.2 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 1002
 storm-constrain control shutdown
 #
 service-instance 1
  encapsulation s-vid 1002
  statistics enable
  xconnect vsi vsi1
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 13.1.1.1 255.255.255.0
#
interface Vsi-interface1
 ip binding vpn-instance vpn1
 ip address 10.255.255.254 255.0.0.0
 mac-address 0000-0001-0001
#
interface Vsi-interface2
 ip binding vpn-instance vpn1
 l3-vni 10000
#
bgp 65000
 peer 172.16.10.1 as-number 65000
 peer 172.16.10.1 connect-interface LoopBack0
 peer 172.16.10.1 password cipher $c$3$saE3frSy9IuWBPp1FJT7L952YRagb0D9Ioo=
 #
 address-family l2vpn evpn
```

```
  peer 172.16.10.1 enable
#
return
```

- RR:

```
#
 sysname RR
#
 router id 172.16.10.1
#
ospf 1
 area 0.0.0.0
  network 12.1.1.0 0.0.0.255
  network 13.1.1.0 0.0.0.255
  network 172.16.10.1 0.0.0.0
#
interface LoopBack0
 ip address 172.16.10.1 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 12.1.1.3 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 13.1.1.3 255.255.255.0
#
bgp 65000
 group leaf internal
 peer leaf connect-interface LoopBack0
 peer leaf password cipher $c$3$91PuaavWEYHlqhaILQV5i5G828J3vG+g67I=
 peer 172.16.0.1 group leaf
 peer 172.16.0.2 group leaf
 #
 address-family l2vpn evpn
  undo policy vpn-target
  peer leaf enable
  peer leaf reflect-client
#
return
```

Contents

Introduction

This document provides examples for configuring priority marking, priority mapping, and queue scheduling profiles.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of priority marking, priority mapping, and queue scheduling profiles.

Example: Configuring priority marking and queue scheduling

Network configuration

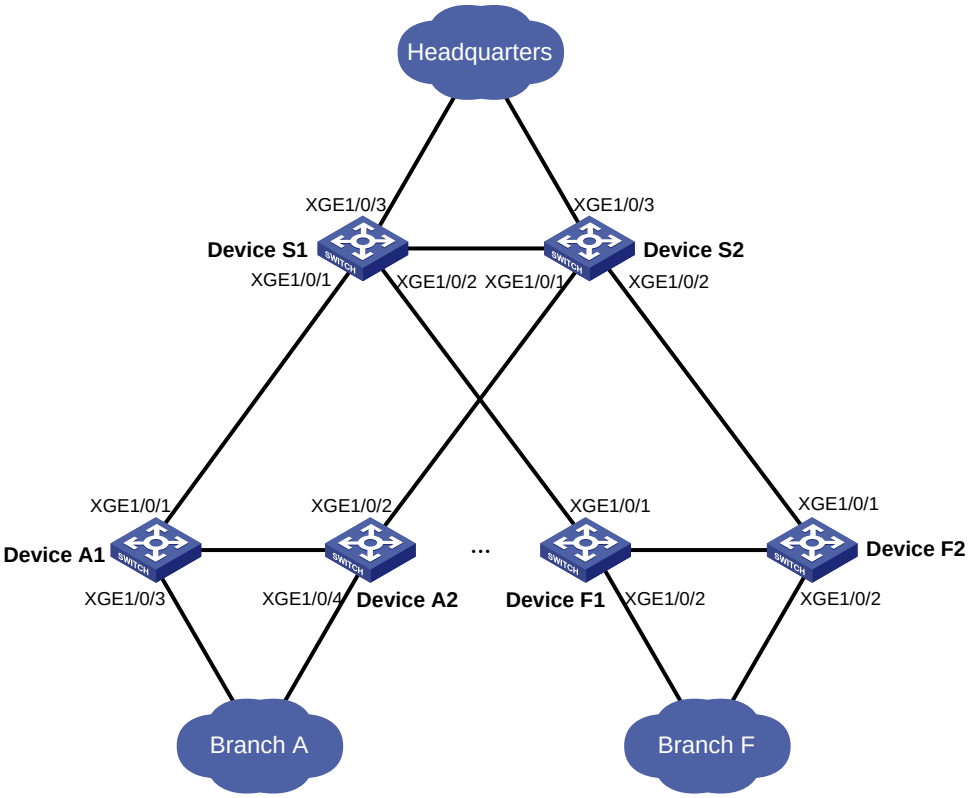
As shown in Figure 1, a company uses dual uplinks to interconnect its headquarters and branches.

The company uses three service types in its intranets:

- **Video service**—Uses network segment 10.1.0.0/16 (10.1.1.0/24 for the headquarters, 10.1.2.0/24 for branch A, 10.1.3.0/24 for branch B, 10.1.4.0/24 for branch C, 10.1.5.0/24 for branch D, 10.1.6.0/24 for branch E, and 10.1.7.0/24 for branch F).
- **Production service**—Uses network segment 10.2.0.0/16 (10.2.1.0/24 for the headquarters, 10.2.2.0/24 for branch A, 10.2.3.0/24 for branch B, 10.2.4.0/24 for branch C, 10.2.5.0/24 for branch D, 10.2.6.0/24 for branch E, and 10.2.7.0/24 for branch F).
- **Voice service**—Uses network segment 10.3.0.0/16 (10.3.1.0/24 for the headquarters, 10.3.2.0/24 for branch A, 10.3.3.0/24 for branch B, 10.3.4.0/24 for branch C, 10.3.5.0/24 for branch D, 10.3.6.0/24 for branch E, and 10.3.7.0/24 for branch F).

Configure priority marking and queue scheduling so the video service, production service, and voice service are scheduled at a ratio of 2:1:1 when congestion occurs.

Figure 1 Network diagram



Analysis

To configure priority marking and queue scheduling, you must perform the following tasks:

- To assign different traffic types to different queues, mark different local precedence values for the service types.
- To schedule the three services at a ratio of 2:1:1, assign their queues to one WRR group and configure weights for these queues.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Release 8106Pxx
S5570S-EI switch series	Release 11xx
S5560X-EI switch series	Release 6628Pxx

S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx
S5500V3-24P-SI switch S5500V3-48P-SI switch	Release 63xx
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI switch series	Release 11xx
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Release 63xx
S5120V2-SI switch series S5120V2-LI switch series	Release 63xx
S5120V3-EI switch series	Release 11xx
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Release 11xx
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI switch series	Release 63xx
S3600V3-EI switch series	Release 11xx
S3600V3-SI switch series	Release 11xx
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx
S5110V2 switch series	Release 63xx
S5110V2-SI switch series	Release 63xx

S5000V3-EI switch series S5000V5-EI switch series	Release 63xx
S5000E-X switch series S5000X-EI switch series	Release 63xx
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Release 63xx
WS5850-WiNet switch series	Release 63xx
WS5820-WiNet switch series WS5810-WiNet switch series	Release 63xx
WAS6000 switch series	Release 63xx
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Release 63xx
IE4520 switch series	Release 66xx
S5135S-EI switch series	Release 6810 and later

Restrictions and guidelines

Marking the DSCP, EXP, 802.1p, IP precedence, or local precedence conflicts with the following actions:

- Traffic filtering (**`filter deny`**).
- Traffic redirecting to the CPU (**`redirect cpu`**).
- Mapping packet colors to drop priority values (**`primap color-map-dp`**).

Procedures

Configuring Device SI

1. Configure a QoS policy on Ten-GigabitEthernet 1/0/3 to assign different traffic types to different queues:

   # Create ACL 3000 to match video traffic, and create a behavior to mark the video traffic with local precedence 2.

   ```
   <DeviceS1> system-view
   [DeviceS1] acl advanced 3000
   [DeviceS1-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255
   destination 10.1.0.0 0.0.255.255
   ```

```
[DeviceS1-acl-ipv4-adv-3000] quit
[DeviceS1] traffic classifier video
[DeviceS1-classifier-video] if-match acl 3000
[DeviceS1-classifier-video] quit
[DeviceS1] traffic behavior video
[DeviceS1-behavior-video] remark local-precedence 2
[DeviceS1-behavior-video] quit
```

Create ACL 3001 to match production traffic, and create a behavior to mark the production traffic with local precedence 3.

```
[DeviceS1] acl advanced 3001
[DeviceS1-acl-ipv4-adv-3001] rule 0 permit ip source 10.2.1.0 0.0.0.255
destination 10.2.0.0 0.0.255.255
[DeviceS1-acl-ipv4-adv-3001] quit
[DeviceS1] traffic classifier production
[DeviceS1-classifier-production] if-match acl 3001
[DeviceS1-classifier-production] quit
[DeviceS1] traffic behavior production
[DeviceS1-behavior-production] remark local-precedence 3
[DeviceS1-behavior-production] quit
```

Create ACL 3002 to match voice traffic, and create a behavior to mark the voice traffic with local precedence 4.

```
[DeviceS1] acl advanced 3002
[DeviceS1-acl-ipv4-adv-3002] rule 0 permit ip source 10.3.1.0 0.0.0.255
destination 10.3.0.0 0.0.255.255
[DeviceS1-acl-ipv4-adv-3002] quit
[DeviceS1] traffic classifier voice
[DeviceS1-classifier-voice] if-match acl 3002
[DeviceS1-classifier-voice] quit
[DeviceS1] traffic behavior voice
[DeviceS1-behavior-voice] remark local-precedence 4
[DeviceS1-behavior-voice] quit
```

Create a QoS policy named **policy1**, and associate the three traffic classes with their respective traffic behaviors.

```
[DeviceS1] qos policy policy1
[DeviceS1-qospolicy-policy1] classifier video behavior video
[DeviceS1-qospolicy-policy1] classifier production behavior production
[DeviceS1-qospolicy-policy1] classifier voice behavior voice
[DeviceS1-qospolicy-policy1] quit
```

Apply the QoS policy **policy1** to the inbound direction of Ten-GigabitEthernet 1/0/3.

```
[DeviceS1] interface ten-gigabitethernet 1/0/3
[DeviceS1-Ten-GigabitEthernet1/0/3] qos apply policy policy1 inbound
[DeviceS1-Ten-GigabitEthernet1/0/3] quit
```

2. Configure a queue scheduling profile on Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2:

Create a queue scheduling profile named **qm1** for WRR. Configure the weights of queue 2 (for video traffic), queue 3 (for production traffic), and queue 4 (for voice traffic) as 2, 1, and 1, respectively.

```
[DeviceS1] qos qmprofile qm1
[DeviceS1-qmprofile-qm1] queue 2 wrr group 1 weight 2
```

```
[DeviceS1-qmprofile-qm1] queue 3 wrr group 1 weight 1
[DeviceS1-qmprofile-qm1] queue 4 wrr group 1 weight 1
[DeviceS1-qmprofile-qm1] quit
```

Apply the queue scheduling profile **qm1** to Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.

```
[DeviceS1] interface ten-gigabitethernet 1/0/1
[DeviceS1-Ten-GigabitEthernet1/0/1] qos apply qmprofile qm1
[DeviceS1-Ten-GigabitEthernet1/0/1] quit
[DeviceS1] interface ten-gigabitethernet 1/0/2
[DeviceS1-Ten-GigabitEthernet1/0/2] qos apply qmprofile qm1
[DeviceS1-Ten-GigabitEthernet1/0/2] quit
```

Configuring Device S2

Configure Device S2 in the same way Device S1 is configured. (Details not shown.)

Configuring Device A1

1. Configure a QoS policy on Ten-GigabitEthernet 1/0/3 to assign different traffic types to different queues:

Create ACL 3000 to match video traffic, and create a behavior to mark the video traffic with local precedence 2.

```
<Device A1> system-view
[DeviceA1] acl advanced 3000
[DeviceA1-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.2.0 0.0.0.255
destination 10.1.0.0 0.0.255.255
[DeviceA1-acl-ipv4-adv-3000] quit
[DeviceA1] traffic classifier video
[DeviceA1-classifier-video] if-match acl 3000
[DeviceA1-classifier-video] quit
[DeviceA1] traffic behavior video
[DeviceA1-behavior-video] remark local-precedence 2
[DeviceA1-behavior-video] quit
```

Create ACL 3001 to match production traffic, and create a behavior to mark the production traffic with local precedence 3.

```
[DeviceA1] acl advanced 3001
[DeviceA1-acl-ipv4-adv-3001] rule 0 permit ip source 10.2.2.0 0.0.0.255
destination 10.2.0.0 0.0.255.255
[DeviceA1-acl-ipv4-adv-3001] quit
[DeviceA1] traffic classifier production
[DeviceA1-classifier-production] if-match acl 3001
[DeviceA1-classifier-production] quit
[DeviceA1] traffic behavior production
[DeviceA1-behavior-production] remark local-precedence 3
[DeviceA1-behavior-production] quit
```

Create ACL 3002 to match voice traffic, and create a behavior to mark the voice traffic with local precedence 4.

```
[DeviceA1] acl advanced 3002
```

```
[DeviceA1-acl-ipv4-adv-3002] rule 0 permit ip source 10.3.2.0 0.0.0.255
destination 10.3.0.0 0.0.255.255
[DeviceA1-acl-ipv4-adv-3002] quit
[DeviceA1] traffic classifier voice
[DeviceA1-classifier-voice] if-match acl 3002
[DeviceA1-classifier-voice] quit
[DeviceA1] traffic behavior voice
[DeviceA1-behavior-voice] remark local-precedence 4
[DeviceA1-behavior-voice] quit
```

Create a QoS policy named **policy1**, and associate the three classes of traffic with their respective traffic behaviors.

```
[DeviceA1] qos policy policy1
[DeviceA1-qospolicy-policy1] classifier video behavior video
[DeviceA1-qospolicy-policy1] classifier production behavior production
[DeviceA1-qospolicy-policy1] classifier voice behavior voice
[DeviceA1-qospolicy-policy1] quit
```

Apply the QoS policy **policy1** to the inbound direction of Ten-GigabitEthernet 1/0/3.

```
[DeviceA1] interface ten-gigabitethernet 1/0/3
[DeviceA1-Ten-GigabitEthernet1/0/3] qos apply policy policy1 inbound
[DeviceA1-Ten-GigabitEthernet1/0/3] quit
```

2. Configure a queue scheduling profile on Ten-GigabitEthernet 1/0/1:

Create a queue scheduling profile named **qm1** for WRR. Configure the weights of queue 2 (for video traffic), queue 3 (for production traffic), and queue 4 (for voice traffic) as 2, 1, and 1, respectively.

```
[DeviceA1] qos qmprofile qm1
[DeviceA1-qmprofile-qm1] queue 2 wrr group 1 weight 2
[DeviceA1-qmprofile-qm1] queue 3 wrr group 1 weight 1
[DeviceA1-qmprofile-qm1] queue 4 wrr group 1 weight 1
[DeviceA1-qmprofile-qm1] quit
```

Apply the queue scheduling profile **qm1** to Ten-GigabitEthernet 1/0/1.

```
[DeviceA1] interface ten-gigabitethernet 1/0/1
[DeviceA1-Ten-GigabitEthernet1/0/1] qos apply qmprofile qm1
[DeviceA1-Ten-GigabitEthernet1/0/1] quit
```

Configuring other devices

Configure Device A2, Device F1, and Device F2 in the same way Device A1 is configured. (Details not shown.)

Verifying the configuration

Verify the configuration on any device, for example, Device S1.

Verify the QoS policy applied to Ten-GigabitEthernet 1/0/3.

```
[DeviceS1] display qos policy interface ten-gigabitethernet 1/0/3
  Interface: Ten-GigabitEthernet1/0/3
  Direction: Inbound
  Policy: policy1
   Classifier: video
```

```
    Operator: AND
    Rule(s) :
     If-match acl 3000
    Behavior: video
     Marking:
       Remark local-precedence 2
  Classifier: production
    Operator: AND
    Rule(s) :
     If-match acl 3001
    Behavior: production
     Marking:
       Remark local-precedence 3
  Classifier: voice
    Operator: AND
    Rule(s) :
     If-match acl 3002
    Behavior: voice
     Marking:
       Remark local-precedence 4
```

Verify the configuration of queue scheduling profiles.

```
[DeviceS1] display qos qmprofile configuration
Queue management profile: qm1 (ID 1)
 Queue ID    Type    Group    Schedule-unit    Schedule-value    Bandwidth
-------------------------------------------------------------------------------
 be          SP      N/A      N/A              N/A                N/A
 af1         SP      N/A      N/A              N/A                N/A
 af2         WRR     1        weight           2                  N/A
 af3         WRR     1        weight           1                  N/A
 af4         WRR     1        weight           1                  N/A
 ef          SP      N/A      N/A              N/A                N/A
 cs6         SP      N/A      N/A              N/A                N/A
 cs7         SP      N/A      N/A              N/A                N/A
```

Configuration files

- Device S1:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
```

```
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.1.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.1.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

- Device S2:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
```

```
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.1.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.1.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

- Device A1:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
```

```
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.2.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

- Device A2:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
```

```
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.2.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

- Device F1:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
```

```
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.7.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.7.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.7.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

- Device F2:

```
#
qos qmprofile qm1
 queue af2 wrr group 1 weight 2
```

```
 queue af3 wrr group 1 weight 1
 queue af4 wrr group 1 weight 1
#
traffic classifier production operator and
 if-match acl 3001
#
traffic classifier video operator and
 if-match acl 3000
#
traffic classifier voice operator and
 if-match acl 3002
#
traffic behavior production
 remark local-precedence 3
#
traffic behavior video
 remark local-precedence 2
#
traffic behavior voice
 remark local-precedence 4
#
qos policy policy1
 classifier video behavior video
 classifier production behavior production
 classifier voice behavior voice
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 qos apply qmprofile qm1
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 qos apply policy policy1 inbound
#
acl advanced 3000
 rule 0 permit ip source 10.1.7.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
#
acl advanced 3001
 rule 0 permit ip source 10.2.7.0 0.0.0.255 destination 10.2.0.0 0.0.255.255
#
acl advanced 3002
 rule 0 permit ip source 10.3.7.0 0.0.0.255 destination 10.3.0.0 0.0.255.255
#
return
```

Contents

Introduction

This document describes typical configurations for EAA.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes you are familiar with EAA features. For the same requirement, the implementation effects of TCL and CLI monitoring strategies are consistent. You can choose either strategy based on preference.

Example: Configuring an EAA TCL monitoring policy

Network configuration

Configure a TCL monitoring policy for the device to execute the following actions when the incoming traffic on Ten-GigabitEthernet1/0/1 reaches or exceeds 500 Mbps:

- Generate logs for traffic that exceeds the range.
- Display the current CPU state and save it to a file.
- Display the state of Ten-GigabitEthernet1/0/1 and save it to a file.

If the subsequent incoming traffic reaches or exceeds 200Mbps, monitoring will restart. When the incoming traffic on the interface is detected to exceed 500Mbps again, the aforementioned operations are executed again.

Applicable hardware and software versions

Table 1 Applicable hardware and software versions

Product	Software version
S6812 series S6813 series	Release 6628Pxx
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Release 8106Pxx
S5570S-EI series	Release 11xx
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx
MS4520V2-30F	Release 6628Pxx

Product	Software version
MS4520V2-30C MS4520V2-54C	Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI series S6520X-EI series	Release 6628Pxx
S6520X-SI series S6520-SI series	Release 6628Pxx
S5000-EI series	Release 6628Pxx
MS4600 series	Release 6628Pxx
ES5500 series	Release 6628Pxx
S5560S-EI series S5560S-SI series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI series	Release 11xx
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Release 63xx
S5120V2-SI series S5120V2-LI series	Release 63xx
S5120V3-EI series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI series	Release 63xx
S3600V3-EI series	Release 11xx
S3600V3-SI series	Release 11xx
S3100V3-EI series S3100V3-SI series	Release 63xx
S5110V2 series	Release 63xx
S5110V2-SI series	Release 63xx
S5000V3-EI series S5000V5-EI series	Release 63xx

Product	Software version
S5000E-X series S5000X-EI series	Release 63xx
E128C E152C E500C series E500D series	Release 63xx
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Release 63xx
WS5850-WiNet series	Release 63xx
WS5820-WiNet series WS5810-WiNet series	Release 63xx
WAS6000 series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Release 63xx
IE4520 series	IE4520 series
S5135S-EI series	Release 6810 and later versions

Procedures

Editing the TCL script

Use Notepad to edit the **test.tcl** file as follows:

Define the monitored event. Configure interface Ten-GigabitEthernet1/0/1 to focus on inbound traffic. When the inbound traffic reaches or exceeds 500 Mbps, configure the device to execute the specified action. The condition to re-enable polling is when the interface traffic reaches or exceeds 200Mbps.

```
::comware::rtm::event_register interface ten-gigabitethernet1/0/1 monitor-obj rcv-bps start-op ge start-val 500000000 restart-op ge restart-val 200000000 user-role network-admin
```

Configure the action to take when the monitored event occurs: Send log message **XGE1/0/1 input rate exceeded 500000000bps** with priority level 1 and device number **local1**.

```
::comware::rtm::action syslog priority 1 facility local1 msg "XGE1/0/1 input rate exceeded 500000000bps"
```

Create the execution action for the monitored event.

```
::comware::create-cli
```

Configure the device to execute the **display cpu-usage** command to display CPU usage statistics and save the information in XGE0_info.txt when the event occurs.

```
::comware::write-cli cli0 "display cpu-usage >> XGE0_info.txt"
```

Configure the device to execute the **display interface ten-gigabitetherne 1/0/1** command to display the current operating state and related information of Ten-GigabitEthernet1/0/1 and save the information in XGE0_info.txt when the event occurs.

```
::comware::write-cli cli0 "display interface ten-gigabitethernet1/0/1 >> XGE0_info.txt"
::comware::write-cli cli0 "end"
```

Configuring the device

Configure the IP address of Ten-GigabitEthernet1/0/1.

```
<Device> system-view
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-mode route
[Device-Ten-GigabitEthernet1/0/1] ip address 192.168.100.66 255.255.255.0
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] quit
```

Download test.tcl to the device through TFTP.

```
<Device> tftp 192.168.100.14 get test.tcl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   189  100   189    0     0   7900      0 --:--:-- --:--:-- --:--:-- 12600
```

Create and enable a TCL monitoring policy, and bind the policy to TCL script **test.tcl**.

```
<Device> system-view
[Device] rtm tcl-policy test test.tcl
[Device] quit
```

Verifying the configuration

Use the **display rtm policy registered** command to view the policy named **test** with the type **Tcl**.

```
<Device> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered        PolicyName
TCL   INTERFACE  May 05 06:46:20 2019  test
```

When the inbound traffic on interface Ten-GigabitEthernet1/0/1 reaches or exceeds 500 Mbps, check all files and folder information in the device for the existence of XGE0_info.txt.

```
<Device> dir
Directory of cfa0:
   0 -rw-        3227 Nov 19 2019 17:28:36   1.cfg
   1 -rw-        2296 Apr 26 2019 18:55:08   5660_data.ak
   2 -rw-        2304 Apr 26 2019 18:54:56   5660_security.ak
   3 -rw-        2298 Apr 26 2019 18:55:16   5660_voice.ak
   4 -rw-        3227 Nov 19 2019 17:15:19   STARTUP110.CFG
   5 drw-           - Mar 10 2019 04:10:10   diagfile
   6 -rw-         567 Jul 17 2019 14:25:00   dsakey
   7 -rw-         223 Jul 17 2019 14:25:00   ecdsakey
   8 -rw-         278 Jul 17 2019 14:25:00   XGE0_info.txt
   9 -rw-         735 Jul 17 2019 14:25:00   hostkey
  10 -rw-         492 Nov 18 2019 16:40:50   ifindex.dat
```

```
  11 -rw-         276 Apr 23 2019 19:00:00   lauth.dat
  12 drw-           - Jul 17 2019 11:26:34   license
  13 drw-           - Apr 24 2019 12:39:38   logfile
  14 -rw-    18839552 Nov 14 2019 16:42:12   msr56-cmw710-boot-r000706.bin
  15 -rw-     1150976 Nov 14 2019 16:43:00   msr56-cmw710-data-r000706.bin
  16 -rw-    47470592 Nov 14 2019 16:42:24   msr56-cmw710-system-r000706.bin
  17 -rw-     2975744 Nov 14 2019 16:42:56   msr56-cmw710-voice-r000706.bin
  18 -rw-    70445056 Nov 14 2019 17:41:08   msr56.ipe
  19 -rw-    70445056 Nov 14 2019 16:40:00   msr56NN.ipe
  20 drw-           - Aug 21 2019 16:23:10   pkey
  21 -rw-         189 Nov 19 2019 17:49:34   test.tcl
  22 drw-           - Mar 10 2019 04:10:10   seclog
  23 -rw-         591 Jul 17 2019 14:25:00   serverkey
  24 -rw-        3227 Nov 18 2019 16:40:50   startup.cfg

507492 KB total (298412 KB free)
```

Use the TFTP method to copy file XGE0_info.txt to the TFTP server.

```
<Device> tftp 192.168.100.14 put XGE0_info.txt
```

View file XGE0_info.txt to display the current state of the CPU and interface Ten-GigabitEthernet1/0/1.

```
Unit CPU usage:
      15% in last 5 seconds
      14% in last 1 minute
      13% in last 5 minutes

Ten-GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description:  Ten-GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet address: 192.168.100.66/24 (primary)
IP packet frame type: Ethernet II, hardware address: 5cdd-7000-a07c
IPv6 packet frame type: Ethernet II, hardware address: 5cdd-7000-a07c
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, Full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Last link flapping: 0 hours 0 minutes 14 seconds
Last clearing of counters: Never
 Peak input rate: 4 bytes/sec, at 2019-09-21 15:09:37
```

```
 Peak output rate: 1 bytes/sec, at 2019-09-21 15:09:37
 Last 300 seconds input rate: 568710000.25 bytes/sec, 64970 bits/sec, 4.96 packets/sec
 Last 300 seconds output rate: 568710000.25 bytes/sec, 64970 bits/sec, 4.96 packets/sec
Input (total):  1703 packets, 2336882000 bytes
          0 unicasts, 0 broadcasts, 4 multicasts, 0 pauses
 Input (normal):  1703 packets, - bytes
          0 unicasts, 0 broadcasts, 4 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 1706 packets,  2337062000 bytes
          0 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 1706 packets, - bytes
          0 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

Configuration files

- Script text for test.tcl:

  ```
  ::comware::rtm::event_register interface ten-gigabitethernet1/0/1 monitor-obj rcv-bps start-op ge start-val 500000000 restart-op ge restart-val 200000000 user-role network-admin
  ::comware::rtm::action syslog priority 1 facility local1 msg "XGE1/0/1 input rate exceeded 500000000bps"
  ::comware::create-cli
  ::comware::write-cli cli0 "display cpu-usage >> XGE0_info.txt"
  ::comware::write-cli cli0 "display interface ten-gigabitethernet1/0/1 >> XGE0_info.txt"
  ::comware::write-cli cli0 "end"
  ```

- Device:

  ```
  #
  interface Ten-GigabitEthernet1/0/1
   port link-mode route
   ip address 192.168.100.66 255.255.255.0
  #
  rtm tcl-policy test test.tcl
  #
  ```

Example: Configuring an EAA CLI monitoring policy

Network configuration

Configure a CLI monitoring policy for the device to execute the following actions when the incoming traffic on Ten-GigabitEthernet1/0/1 reaches or exceeds 500 Mbps:

- Generate logs for traffic that exceeds the range.
- Display the current CPU state and save it to a file.
- Display the state of Ten-GigabitEthernet1/0/1 and save it to a file.

If the subsequent incoming traffic reaches or exceeds 200Mbps, monitoring will restart. When the incoming traffic on the interface is detected to exceed 500Mbps again, the aforementioned operations are executed again.

Applicable hardware and software versions

Table 2 Applicable hardware and software versions

Product	Software version
S6812 series S6813 series	Release 6628Pxx
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Release 8106Pxx
S5570S-EI series	Release 11xx
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx
MS4520V2-30F	Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI series S6520X-EI series	Release 6628Pxx
S6520X-SI series S6520-SI series	Release 6628Pxx
S5000-EI series	Release 6628Pxx
MS4600 series	Release 6628Pxx
ES5500 series	Release 6628Pxx
S5560S-EI series S5560S-SI series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI series	Release 11xx
S5130S-HI series S5130S-EI series	Release 63xx

Product	Software version
S5130S-SI series S5130S-LI series	
S5120V2-SI series S5120V2-LI series	Release 63xx
S5120V3-EI series	Release 11xx
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Release 11xx
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI series	Release 63xx
S3600V3-EI series	Release 11xx
S3600V3-SI series	Release 11xx
S3100V3-EI series S3100V3-SI series	Release 63xx
S5110V2 series	Release 63xx
S5110V2-SI series	Release 63xx
S5000V3-EI series S5000V5-EI series	Release 63xx
S5000E-X series S5000X-EI series	Release 63xx
E128C E152C E500C series E500D series	Release 63xx
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Release 63xx
WS5850-WiNet series	Release 63xx
WS5820-WiNet series WS5810-WiNet series	Release 63xx
WAS6000 series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Release 63xx
IE4520 series	IE4520 series
S5135S-EI series	Release 6810 and later versions

Restrictions and guidelines

- For a policy, you can configure only one trigger event and one running time. When you repeatedly execute the **`event or running-time`** commands, the most recently configured and committed changes take effect.
- If the number of the newly configured action matches an existing action number, execute the **`commit`** command for the most recent configuration to take effect.
- After configuring the event, action, user role, and running time for the CLI monitoring policy, you must execute the **`commit`** command to enable the policy and activate its configurations.

Procedures

Configure the IP address of Ten-GigabitEthernet1/0/1.

```
<Device> system-view
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port link-mode route
[Device-Ten-GigabitEthernet1/0/1] ip address 192.168.100.66 255.255.255.0
[Device-Ten-GigabitEthernet1/0/1] quit
```

Create CLI policy 1.

```
[Device] rtm cli-policy 1
```

Configure the monitored event. Configure the device to execute the specified action when the inbound traffic on interface Ten-GigabitEthernet1/0/1 reaches or exceeds 500 Mbps. The condition to re-enable polling is when the interface traffic reaches or exceeds 200Mbps.

```
[Device-rtm-1] event interface ten-gigabitethernet 1/0/1 monitor-obj rcv-bps start-op ge start-val 500000000 restart-op ge restart-val 200000000
```

Configure the action to take when the monitored event occurs: Send log message **XGE1/0/1 input rate exceeded 500000000bps** with priority level 1 and log recording tool **local1**.

```
[Device-rtm-1] action 1 syslog priority 1 facility local1 msg "XGE1/0/1 input rate exceeded 500000000bps"
```

Configure the device to execute the **`display cpu-usage`** command to display CPU usage statistics and save the information in XGE0_info.txt when the event occurs.

```
[Device-rtm-1] action 2 cli display cpu-usage >> XGE0_info.txt
```

Configure the device to execute the **`display interface ten-gigabitetherne 1/0/1`** command to display the current operating state and related information of Ten-GigabitEthernet1/0/1 and save the information in XGE0_info.txt when the event occurs.

```
[Device-rtm-1] action 3 cli display interface ten-gigabitethernet 1/0/1 >> XGE0_info.txt
```

Set the policy running time to 30 seconds.

```
[Device-rtm-1] running-time 30
```

Specify user role **network-admin** for the execution of CLI monitoring policy 1.

```
[Device-rtm-1] user-role network-admin
```

Enable CLI monitoring policy 1.

```
[Device-rtm-1] commit
[Device-rtm-1] quit
```

Verifying the configuration

Use the **display rtm policy registered** command to view policy 1 with the type **CLI**.

```
<Device> display rtm policy registered
Total number: 1
Type  Event      TimeRegistered        PolicyName
CLI   INTERFACE  May 04 00:12:40 2019  1
```

When the inbound traffic on interface Ten-GigabitEthernet1/0/1 reaches or exceeds 500 Mbps, check all files and folder information in the device for the existence of XGE0_info.txt.

```
<Device> dir
Directory of cfa0:
   0 -rw-        3227 Nov 19 2019 17:28:36   1.cfg
   1 -rw-        2296 Apr 26 2019 18:55:08   5660_data.ak
   2 -rw-        2304 Apr 26 2019 18:54:56   5660_security.ak
   3 -rw-        2298 Apr 26 2019 18:55:16   5660_voice.ak
   4 -rw-        3227 Nov 19 2019 17:15:19   STARTUP110.CFG
   5 drw-           - Mar 10 2019 04:10:10   diagfile
   6 -rw-         567 Jul 17 2019 14:25:00   dsakey
   7 -rw-         223 Jul 17 2019 14:25:00   ecdsakey
   8 -rw-         278 Jul 17 2019 14:25:00   XGE0_info.txt
   9 -rw-         735 Jul 17 2019 14:25:00   hostkey
  10 -rw-         492 Nov 18 2019 16:40:50   ifindex.dat
  11 -rw-         276 Apr 23 2019 19:00:00   lauth.dat
  12 drw-           - Jul 17 2019 11:26:34   license
  13 drw-           - Apr 24 2019 12:39:38   logfile
  14 -rw-    18839552 Nov 14 2019 16:42:12   msr56-cmw710-boot-r000706.bin
  15 -rw-     1150976 Nov 14 2019 16:43:00   msr56-cmw710-data-r000706.bin
  16 -rw-    47470592 Nov 14 2019 16:42:24   msr56-cmw710-system-r000706.bin
  17 -rw-     2975744 Nov 14 2019 16:42:56   msr56-cmw710-voice-r000706.bin
  18 -rw-    70445056 Nov 14 2019 17:41:08   msr56.ipe
  19 -rw-    70445056 Nov 14 2019 16:40:00   msr56NN.ipe
  20 drw-           - Aug 21 2019 16:23:10   pkey
  21 -rw-         189 Nov 19 2019 17:49:34   test.tcl
  22 drw-           - Mar 10 2019 04:10:10   seclog
  23 -rw-         591 Jul 17 2019 14:25:00   serverkey
  24 -rw-        3227 Nov 18 2019 16:40:50   startup.cfg


507492 KB total (298412 KB free)
```

Use the TFTP method to copy file XGE0_info.txt to the TFTP server.

```
<Device> tftp 192.168.100.14 put XGE0_info.txt
```

View file XGE0_info.txt to display the current state of the CPU and interface Ten-GigabitEthernet1/0/1.

```
Unit CPU usage:
      15% in last 5 seconds
      14% in last 1 minute
      13% in last 5 minutes
```

```
Ten-GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
Description:  Ten-GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet address: 192.168.100.66/24 (primary)
IP packet frame type: Ethernet II, hardware address: 5cdd-7000-a07c
IPv6 packet frame type: Ethernet II, hardware address: 5cdd-7000-a07c
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 0
1000Mbps-speed mode, Full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Last link flapping: 0 hours 0 minutes 14 seconds
Last clearing of counters: Never
 Peak input rate: 4 bytes/sec, at 2019-09-21 15:09:37
 Peak output rate: 1 bytes/sec, at 2019-09-21 15:09:37
 Last 300 seconds input rate: 568710000.25 bytes/sec, 64970 bits/sec, 4.96 packets/sec
 Last 300 seconds output rate: 568710000.25 bytes/sec, 64970 bits/sec, 4.96 packets/sec
Input (total):  1703 packets, 2336882000 bytes
          0 unicasts, 0 broadcasts, 4 multicasts, 0 pauses
 Input (normal):  1703 packets, - bytes
          0 unicasts, 0 broadcasts, 4 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 1706 packets,  2337062000 bytes
          0 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 1706 packets, - bytes
          0 unicasts, 5 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

Configuration files

```
#
interface Ten-GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.100.66 255.255.255.0
#
```

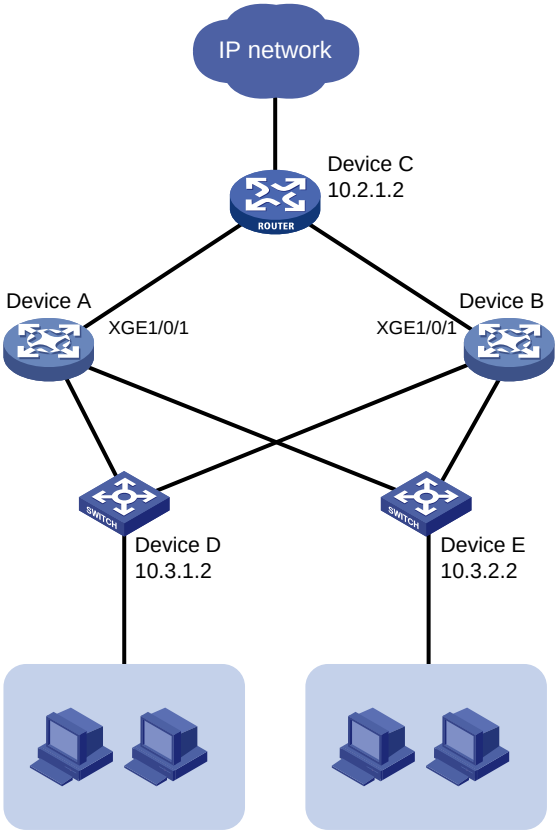
```
rtm cli-policy 1
 event interface Ten-GigabitEthernet1/0/1 monitor-obj rcv-bps start-op ge start-val
500000000 restart-op ge restart-val 200000000
 action 1 syslog priority 1 facility local1 msg "XGE1/0/1 input rate exceeded 500000000bps"
 action 2 cli display cpu-usage >> XGE0_info.txt
 action 3 cli display interface ten-gigabitethernet 1/0/1 >> XGE0_info.txt
 running-time 30
 user-role network-admin
#
```

Example: Configuring EAA and track entry association

Network configuration

Device A has established BGP sessions with Device D and Device E. Normally, traffic from Device D and Device E to the Internet is forwarded through Device A. Configure EAA and track entry association to achieve the following: When the state of interface Ten-GigabitEthernet1/0/1 connecting Device A to Device C changes to Down, Device A automatically detects the port down event and blocks BGP sessions with Device D and Device E. Consequently, traffic from Device D and Device E to the external network can be rerouted through Device B.

Figure 1 Network diagram



Applicable hardware and software versions

Table 3 Applicable hardware and software versions

Product	Software version
S6812 series S6813 series	Release 6628Pxx
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Release 8106Pxx
S5570S-EI series	Release 11xx
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx
MS4520V2-30F	Release 6628Pxx
MS4520V2-30C MS4520V2-54C	Release 6628Pxx
MS4520V2-28S MS4520V2-24TP	Release 63xx
S6520X-HI series S6520X-EI series	Release 6628Pxx
S6520X-SI series S6520-SI series	Release 6628Pxx
S5000-EI series	Release 6628Pxx
MS4600 series	Release 6628Pxx
ES5500 series	Release 6628Pxx
S5560S-EI series S5560S-SI series	Release 63xx
S5500V3-24P-SI S5500V3-48P-SI	Release 63xx
S5500V3-SI series (excluding S5500V3-24P-SI and S5500V3-48P-SI)	Release 11xx
S5170-EI series	Release 11xx
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Release 63xx
S5120V2-SI series S5120V2-LI series	Release 63xx
S5120V3-EI series	Release 11xx
S5120V3-36F-SI	Release 11xx

Product	Software version
S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Release 63xx
S5120V3-LI series	Release 63xx
S3600V3-EI series	Release 11xx
S3600V3-SI series	Release 11xx
S3100V3-EI series S3100V3-SI series	Release 63xx
S5110V2 series	Release 63xx
S5110V2-SI series	Release 63xx
S5000V3-EI series S5000V5-EI series	Release 63xx
S5000E-X series S5000X-EI series	Release 63xx
E128C E152C E500C series E500D series	Release 63xx
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Release 63xx
WS5850-WiNet series	Release 63xx
WS5820-WiNet series WS5810-WiNet series	Release 63xx
WAS6000 series	Release 63xx
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Release 63xx
IE4520 series	IE4520 series
S5135S-EI series	Release 6810 and later versions

Procedures

View the current state and statistics of the BGP peers.

```
<DeviceA> display bgp peer ipv4

 BGP local router ID: 1.1.1.1
```

```
 Local AS number: 100
 Total number of peers: 3                 Peers in established state: 3

  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  10.2.1.2                200       13       16    0       0 00:16:12 Established
  10.3.1.2                300       13       16    0       0 00:10:34 Established
  10.3.2.2                300       13       16    0       0 00:10:38 Established
```

Configure a track item to monitor the state of Ten-GigabitEthernet1/0/1.

```
<DeviceA> system-view
[DeviceA] track 1 interface ten-gigabitethernet 1/0/1
```

Configure a TCL monitoring policy for Device A to automatically detect Ten-GigabitEthernet1/0/1 down events and prevent BGP sessions from being established with Device D and Device E.

```
[DeviceA] rtm cli-policy test
[DeviceA-rtm-test] event track 1 state negative
[DeviceA-rtm-test] action 0 cli system-view
[DeviceA-rtm-test] action 1 cli bgp 100
[DeviceA-rtm-test] action 2 cli peer 10.3.1.2 ignore
[DeviceA-rtm-test] action 3 cli peer 10.3.2.2 ignore
[DeviceA-rtm-test] user-role network-admin
[DeviceA-rtm-test] commit
[DeviceA-rtm-test] quit
```

Verifying the configuration

Disable Ten-GigabitEthernet1/0/1.

```
[DeviceA] interface ten-gigabitethernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] shutdown
```

View the state and statistics of BGP peers. Verify that the number of BGP peers is 0.

```
<DeviceA> display bgp peer ipv4
 BGP local router ID: 1.1.1.1
 Local AS number: 100
 Total number of peers: 0                 Peers in established state: 0
  * - Dynamically created peer
  Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State
```

Configuration files

```
#
rtm cli-policy test
 event track 1 state negative
 action 0 cli system-view
 action 1 cli bgp 100
 action 2 cli peer 10.3.1.2 ignore
 action 3 cli peer 10.3.2.2 ignore
 user-role network-operator
```

```
 user-role network-admin
#
track 1 interface ten-gigabitethernet 1/0/1
#
```

Contents

Introduction

In an MPLS L3VPN, a CE is typically connected to a PE directly. In some networks, a direct connection might not be available between a CE and a PE. In such scenarios, you can configure a GRE tunnel between the CE and PE to establish a virtual point-to-point link. This setup allows the CE and PE to communicate as if they were directly connected.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge MPLS L3VPN and GRE.

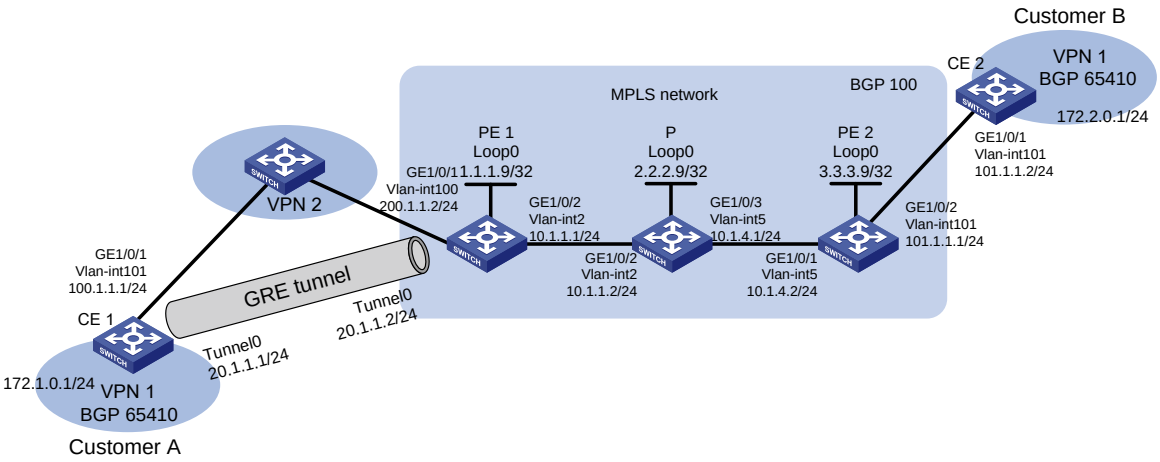
Example: Configuring GRE tunnel access to an MPLS L3VPN

Network configuration

As shown in Figure 1, Customer A and Customer B belong to VPN 1. Deploy an MPLS L3VPN to securely transmit user data between Customer A and Customer B through the VPN.

- PE 1 and PE 2 are edge devices of the MPLS backbone network.
- CE 1 and CE 2 are customer edge devices for VPN 1.
- A network (VPN 2) exists between CE 1 and PE 1. CE 1 and CE 2 are able to route to each other.

Figure 1 Network diagram



Analysis

- To transfer packets on the MPLS network, configure an IGP routing protocol on the MPLS backbone, and use LDP to distribute public network (outer) labels to VPN packets.
- To transport VPN routes and allocate VPN (inner) labels, establish an MP-IBGP peer relationship between the PEs.
- To establish a logical direct connection between CE 1 and PE 1, configure a GRE tunnel between them.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6615Pxx, Release 6628Pxx
S6550XE-HI switch series	Release 6008 and later, Release 8106Pxx
S6525XE-HI switch series	Release 6008 and later, Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560X-HI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5500V2-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-30F switch	Release 65xx, Release 6615Pxx, Release 6628Pxx

Hardware	Software version
MS4520V2-30C switch MS4520V2-54C switch	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4520V2-28S 1 switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5000-EI switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
MS4600 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
ES5500 switch series	Release 65xx, Release 6615Pxx, Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported

Hardware	Software version
S5000E-X switch series S5000X-EI switch series	Not supported
E128C 1 switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch	Not supported

Restrictions and guidelines

When an interface is bound to a VPN instance, the settings (including IP address) on the interface will be cleared. Therefore, bind an interface to a VPN instance before you configure other settings on the interface.

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **`reserve-vlan-interface`** command to reserve local VLAN interface resources. For more information about the **`reserve-vlan-interface`** command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring an IGP on the MPLS backbone

This example uses OSPF to implement IP connectivity between the PE and P devices on the MPLS backbone.

1. Configure PE 1:

   # Configure IP addresses for the loopback interface and the backbone network interfaces.

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] vlan 2
[PE1-vlan2] port GigabitEthernet 1/0/2
[PE1-vlan2] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] quit
```

   # Enable OSPF on the interfaces attached to the backbone network.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

2. Configure P:

   # Configure IP addresses for the loopback interface and the backbone network interfaces.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] vlan 2
[P-vlan2] port GigabitEthernet 1/0/2
[P-vlan2] quit
[P] vlan 5
[P-vlan5] port GigabitEthernet 1/0/3
[P-vlan5] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
[P] interface vlan-interface 5
[P-Vlan-interface5] ip address 10.1.4.1 24
[P-Vlan-interface5] quit
```

   # Enable OSPF on the interfaces attached to the backbone network.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

3. Configure PE 2:

Configure IP addresses for the loopback interface and the backbone network interfaces.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] vlan 5
[PE2-vlan5] port GigabitEthernet 1/0/1
[PE2-vlan5] quit
[PE2] interface vlan-interface 5
[PE2-Vlan-interface5] ip address 10.1.4.2 24
[PE2-Vlan-interface5] quit
```

Enable OSPF on the interfaces attached to the backbone network.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

After the configuration is completed, PE 1, P, and PE 2 can establish OSPF neighbor relationships. Execute the **`display ospf peer`** command to verify that the neighbors are in full state. Execute the **`display ip routing-table`** command to verify that the PEs have learned the routes to the loopback interfaces of each other.

Use PE 1 as an example:

```
[PE1] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.9
                  Neighbors

 Area 0.0.0.0 interface 10.1.1.1(Vlan-interface2)'s neighbors
 Router ID: 2.2.2.9          Address: 10.1.1.2        GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 10.1.1.2  BDR: 10.1.1.1  MTU: 0
   Options is 0x02 (-|-|-|-|-|-|E|-)
   Dead timer due in 38  sec
   Neighbor is up for 17:30:25
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
   BFD status: Disabled
[PE1] display ip routing-table protocol ospf

Summary Count : 5

OSPF Routing table Status : <Active>
Summary Count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.9/32          OSPF   10   1            10.1.1.2        Vlan2
```

```
3.3.3.9/32          OSPF   10   2           10.1.1.2        Vlan2
10.1.4.0/24         OSPF   10   2           10.1.1.2        Vlan2

OSPF Routing table Status : <Inactive>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.9/32          OSPF   10   0           1.1.1.9         Loop0
10.1.1.0/24         OSPF   10   1           10.1.1.1        Vlan2
```

Configuring basic MPLS and MPLS LDP on the MPLS backbone to establish LDP LSPs

1. Configure PE 1:

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls ldp
[PE1-ldp] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] mpls enable
[PE1-Vlan-interface2] mpls ldp enable
[PE1-Vlan-interface2] quit
```

2. Configure P:

```
[P] mpls lsr-id 2.2.2.9
[P] mpls ldp
[P-ldp] quit
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls enable
[P-Vlan-interface2] mpls ldp enable
[P-Vlan-interface2] quit
[P] interface vlan-interface 5
[P-Vlan-interface5] mpls enable
[P-Vlan-interface5] mpls ldp enable
[P-Vlan-interface5] quit
```

3. Configure PE 2:

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls ldp
[PE2-ldp] quit
[PE2] interface vlan-interface 5
[PE2-Vlan-interface5] mpls enable
[PE2-Vlan-interface5] mpls ldp enable
[PE2-Vlan-interface5] quit
```

Execute the **`display mpls ldp peer`** command to verify that LDP sessions in **Operational** state have been established between PE 1, P, and PE 2. Execute the **`display mpls ldp lsp`** command to verify that the LSPs have been established by LDP.

Use PE1 as an example.

```
[PE1] display mpls ldp peer
Total number of peers: 1
Peer LDP ID             State         Role     GR   MD5  KA Sent/Rcvd
2.2.2.9:0               Operational   Passive  Off  Off  5/5
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 4            Ingress: 1          Transit: 1      Egress: 3

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
2.2.2.9/32         -/3                 10.1.1.2        Vlan2
                   1151/3              10.1.1.2        Vlan2
3.3.3.9/32         -/1150              10.1.1.2        Vlan2
                   1150/1150           10.1.1.2        Vlan2
```

Configuring VPN instances on PE 1 and CE 1 and establishing a GRE tunnel to connect CE 1 to PE 1

Configuring VPN instances on PE 1 and CE 1

1. Configure PE 1:

Create a VPN instance named **vpn1** on PE 1.

```
[PE1] ip vpn-instance vpn1
```

Configure the RD of the VPN instance as 100:1.

```
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
```

Configure route targets for the VPN instance.

```
[PE1-vpn-instance-vpn1] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-vpn1] quit
```

Bind VLAN-interface 100 to the VPN instance.

```
[PE1] vlan 100
[PE1-vlan100] port GigabitEthernet 1/0/1
[PE1-vlan100] quit
[PE1] interface vlan-interface 100
[PE1-Vlan-interface100] ip binding vpn-instance vpn1
[PE1-Vlan-interface100] ip address 200.1.1.2 24
[PE1-Vlan-interface100] quit
```

2. Configure CE 1:

Create a VPN instance named **vpn1** on CE 1.

```
[CE1] ip vpn-instance vpn1
```

Configure the RD of the VPN instance as 100:1.

```
[CE1-vpn-instance-vpn1] route-distinguisher 100:1
```

Configure route targets for the VPN instance.

```
[CE1-vpn-instance-vpn1] vpn-target 100:1 import-extcommunity
[CE1-vpn-instance-vpn1] vpn-target 100:1 export-extcommunity
[CE1-vpn-instance-vpn1] quit
```

Bind VLAN-interface 101 to the VPN instance.

```
[CE1] vlan 101
[CE1-vlan101] port GigabitEthernet 1/0/1
[CE1-vlan101] quit
[CE1] interface vlan-interface 101
[CE1-Vlan-interface101] ip binding vpn-instance vpn1
[CE1-Vlan-interface101] ip address 100.1.1.1 24
[CE1-Vlan-interface101] quit
```

Configuring a GRE tunnel between CE 1 and PE 1

1. Configure CE 1:

Create service loopback group 1 and configure the service type as tunnel. Assign interface GigabitEthernet 1/0/3 to service loopback group 1. (For the S6550XE-HI, S6525XE-HI, and S5850 switch series, you must create a tunnel-type service loopback group to enable the reception and transmission of tunnel packets.)

```
[CE1] service-loopback group 1 type tunnel
```

Assign interface GigabitEthernet 1/0/3 to service loopback group 1.

```
[CE1] interface GigabitEthernet 1/0/3
[CE1-GigabitEthernet1/0/3] port service-loopback group 1
[CE1-GigabitEthernet1/0/3] quit
```

Create tunnel interface Tunnel 0, and specify the tunnel mode as GRE/IPv4.

```
[CE1] interface tunnel 0 mode gre
```

Specify a VPN instance for the tunnel source address.

```
[CE1-Tunnel0] ip binding vpn-instance vpn1
```

Assign an IP address to interface Tunnel 0.

```
[CE1-Tunnel0] ip address 20.1.1.1 255.255.255.0
```

Configure the tunnel source address as the IP address of VLAN-interface 101 on CE 1.

```
[CE1-Tunnel0] source vlan-interface 101
```

Configure the tunnel destination address as the IP address of VLAN-interface 100 on PE 1.

```
[CE1-Tunnel0] destination 200.1.1.2
```

Specify a VPN instance for the tunnel destination address.

```
[CE1-Tunnel0] tunnel vpn-instance vpn1
[CE1-Tunnel0] quit
```

Configure a static route for Customer A to reach Customer B via Tunnel 0.

```
[CE1] ip route-static vpn-instance vpn1 172.2.0.0 24 tunnel 0
```

2. Configure PE 1:

Create service loopback group 1 and configure the service type as tunnel. Assign interface GigabitEthernet 1/0/3 to service loopback group 1. (For the S6550XE-HI, S6525XE-HI, and

S5850 switch series, you must create a tunnel-type service loopback group to enable the reception and transmission of tunnel packets.)

```
[PE1] service-loopback group 1 type tunnel
```

Assign interface GigabitEthernet 1/0/3 to service loopback group 1.

```
[PE1] interface GigabitEthernet 1/0/3
[PE1-GigabitEthernet1/0/3] port service-loopback group 1
[PE1-GigabitEthernet1/0/3] quit
```

Create tunnel interface Tunnel 0, and specify the tunnel mode as GRE/IPv4.

```
[PE1] interface tunnel 0 mode gre
```

Specify a VPN instance for the tunnel source address.

```
[PE1-Tunnel0] ip binding vpn-instance vpn1
```

Assign an IP address to interface Tunnel 0.

```
[PE1-Tunnel0] ip address 20.1.1.2 255.255.255.0
```

Configure the tunnel source address as the IP address of VLAN-interface 100 on PE 1.

```
[PE1-Tunnel0] source vlan-interface 100
```

Configure the tunnel destination address as the IP address of VLAN-interface 101 on CE 1.

```
[PE1-Tunnel0] destination 100.1.1.1
```

Specify a VPN instance for the tunnel destination address.

```
[PE1-Tunnel0] tunnel vpn-instance vpn1
[PE1-Tunnel0] quit
```

Configure a static route for Customer B to reach Customer A via Tunnel 0.

```
[PE1] ip route-static vpn-instance vpn1 172.1.0.0 24 Tunnel 0
```

Configuring a VPN instance on PE 2 to allow CE 2 access to PE 2

1. Configure PE 2:

Create a VPN instance named **vpn1** on PE 2.

```
[PE2] ip vpn-instance vpn1
```

Configure an RD of the VPN instance.

```
[PE2-vpn-instance-vpn1] route-distinguisher 100:1
```

Configure the import target and export target for the VPN instance, which must be the same as the export target and import target on PE 1.

```
[PE2-vpn-instance-vpn1] vpn-target 100:1 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 100:1 export-extcommunity
[PE2-vpn-instance-vpn1] quit
```

Bind VLAN-interface 101 to the VPN instance.

```
[PE2] vlan 101
[PE2-vlan101] port GigabitEthernet 1/0/2
[PE2-vlan101] quit
[PE2] interface vlan-interface 101
```

```
[PE2-Vlan-interface101] ip binding vpn-instance vpn1
[PE2-Vlan-interface101] ip address 101.1.1.1 24
[PE2-Vlan-interface101] quit
```

2. Configure CE 2:

   Configure IP addresses for interfaces on CE 2 as shown in Figure 1. (Details not shown.)

   After the configuration is completed, execute the **display ip vpn-instance** command on PE 2 to view the VPN instance configuration. PE 2 can ping the connected CE 2.

```
[PE2] display ip vpn-instance
  Total VPN-Instances configured : 1
  VPN-Instance Name               RD                     Create time
  vpn1                            100:1                  2016/06/22 13:20:08
[PE2] ping -vpn-instance vpn1 101.1.1.2
Ping 10.1.4.2 (101.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 101.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 101.1.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 101.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 101.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 101.1.1.2: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 10.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms
```

Establishing EBGP peers between PEs and CEs to redistributing VPN routes

1. Configure PE 1:

   # Create BGP process 100 on PE 1.

```
[PE1] bgp 100
```

   # Specify CE 1 as the peer. Redistribute the direct routes in the routing table of PE 1 into the routing table of the BGP-VPN instance.

```
[PE1-bgp-default] ip vpn-instance vpn1
[PE1-bgp-default-vpn1] peer 20.1.1.1 as-number 65410
[PE1-bgp-default-vpn1] address-family ipv4 unicast
[PE1-bgp-default-ipv4-vpn1] peer 20.1.1.1 enable
[PE1-bgp-default-ipv4-vpn1] import-route direct
[PE1-bgp-default-ipv4-vpn1] quit
[PE1-bgp-default-vpn1] quit
```

2. Configure PE 2:

   # Create BGP process 100 on PE 2.

```
[PE2] bgp 100
```

Specify CE 2 as the peer. Redistribute the direct routes in the routing table of PE 2 into the routing table of the BGP-VPN instance.

```
[PE2-bgp-default] ip vpn-instance vpn1
[PE2-bgp-default-vpn1] peer 101.1.1.2 as-number 65410
[PE2-bgp-default-vpn1] address-family ipv4 unicast
[PE2-bgp-default-ipv4-vpn1] peer 101.1.1.2 enable
[PE2-bgp-default-ipv4-vpn1] import-route direct
[PE2-bgp-default-ipv4-vpn1] quit
[PE2-bgp-default-vpn1] quit
```

3. Configure CE 1:

Create BGP process 65410 on CE 1. Specify PE 1 as the peer with AS number 100.

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp-default] peer 20.1.1.2 as-number 100
```

Enable CE 1 to exchange IPv4 unicast routing information with peer 20.1.1.2.

```
[CE1-bgp-default] address-family ipv4 unicast
[CE1-bgp-default-ipv4] peer 20.1.1.2 enable
```

Redistribute the direct routes of CE 1 into EBGP.

```
[CE1-bgp-default-ipv4] import-route direct
[CE1-bgp-default-ipv4] quit
[CE1-bgp-default] quit
```

4. Configure CE 2:

Create BGP process 65410 on CE 2. Specify PE 2 as the peer with AS number 100.

```
<CE2> system-view
[CE2] bgp 65410
[CE2-bgp-default] peer 101.1.1.1 as-number 100
```

Enable CE 2 to exchange IPv4 unicast routing information with peer 101.1.1.1.

```
[CE2-bgp-default] address-family ipv4 unicast
[CE2-bgp-default-ipv4] peer 101.1.1.1 enable
```

Redistribute the direct routes of CE 2 into EBGP.

```
[CE2-bgp-default-ipv4] import-route direct
[CE2-bgp-default-ipv4] quit
[CE2-bgp-default] quit
```

Execute the **`display bgp peer ipv4 vpn-instance`** command on PE 2 to verify that PE 2 has a BGP peer in **Established** state with CE 2.

```
[PE2] display bgp peer ipv4 vpn-instance vpn1
 BGP local router ID: 3.3.3.9
 Local AS number: 100
 Total number of peers: 1                 Peers in established state: 1

  Peer                 AS          MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

  101.1.1.2           65430        4        4    0       2 13:35:25     Established
```

Establishing MP-IBGP peers between PEs

1. Configure PE 1:

   # On PE 1, specify PE 2 as the BGP peer, and specify Loopback 0 as the source interface for TCP connections to the peer.

   ```
   [PE1] bgp 100
   [PE1-bgp-default] peer 3.3.3.9 as-number 100
   [PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
   ```

   # Enter BGP VPNv4 address family view, and specify PE 2 as the peer.

   ```
   [PE1-bgp-default] address-family vpnv4
   [PE1-bgp-default-vpnv4] peer 3.3.3.9 enable
   [PE1-bgp-default-vpnv4] quit
   [PE1-bgp-default] quit
   ```

2. Configure PE 2:

   # On PE 2, specify PE 1 as the BGP peer, and specify Loopback 0 as the source interface for TCP connections to the peer.

   ```
   [PE2] bgp 100
   [PE2-bgp-default] peer 1.1.1.9 as-number 100
   [PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
   ```

   # Enter BGP VPNv4 address family view, and specify PE 1 as the peer.

   ```
   [PE2-bgp-default] address-family vpnv4
   [PE2-bgp-default-vpnv4] peer 1.1.1.9 enable
   [PE2-bgp-default-vpnv4] quit
   [PE2-bgp-default] quit
   ```

   # Execute the **`display bgp peer vpnv4`** command to verify that the PEs have BGP peers in **Established** state with each other.

   ```
   [PE1] display bgp peer vpnv4

    BGP local router ID: 1.1.1.9
    Local AS number: 100
    Total number of peers: 1                 Peers in established state: 1

     Peer                    AS  MsgRcvd  MsgSent OutQ PrefRcv Up/Down  State

     3.3.3.9                100        8        8    0       0 00:00:08 Established
   ```

Verifying the configuration

Execute the **`display ip routing-table vpn-instance`** command on a PE to view the route destined to the peer CE.

Use VPN instance **vpn1** on PE 1 as an example:

```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
20.1.1.0/24         Direct  0   0           20.1.1.2        Tun0
20.1.1.0/32         Direct  0   0           20.1.1.2        Tun0
20.1.1.2/32         Direct  0   0           127.0.0.1       InLoop0
200.1.1.0/24        Direct 0    0           200.1.1.2       Vlan100
200.1.1.0/32        Direct 0    0           200.1.1.2       Vlan100
200.1.1.2/32        Direct 0    0           127.0.0.1       InLoop0
200.1.1.255/32      Direct 0    0           100.1.1.2       Vlan100
101.1.1.0/24        BGP    255  0           3.3.3.9         Vlan2
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

Configuration files

- PE 1

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
 service-loopback group 1 type tunnel
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 100
#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
```

```
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface100
 ip binding vpn-instance vpn1
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ip binding vpn-instance vpn1
 ip address 20.1.1.2 255.255.255.0
 source Vlan-interface100
 tunnel vpn-instance vpn1
 destination 100.1.1.1
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 3.3.3.9 enable
 #
 ip vpn-instance vpn1
  peer 20.1.1.1 as-number 65410
  #
  address-family ipv4 unicast
   import-route direct
   peer 20.1.1.1 enable
#
 ip route-static vpn-instance vpn1 172.1.0.0 24 Tunnel0
```

- P

```
#
ospf 1
 area 0.0.0.0
```

```
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 5
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface5
 ip address 10.1.4.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 5
#
```

- PE 2

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.1.4.0 0.0.0.255
#
 mpls lsr-id 3.3.3.9
#
 lldp global enable
```

```
#
vlan 5
#
vlan 101
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface5
 ip address 10.1.4.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface101
 ip binding vpn-instance vpn1
 ip address 101.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 101
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 #
 address-family vpnv4
  peer 1.1.1.9 enable
 #
 ip vpn-instance vpn1
  peer 101.1.1.2 as-number 65410
  #
  address-family ipv4 unicast
   import-route direct
   peer 101.1.1.2 enable
#
```

- CE 1

```
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 import-extcommunity
 vpn-target 100:1 export-extcommunity
#
```

```
 service-loopback group 1 type tunnel
#
vlan 101
#
interface Vlan-interface101
 ip binding vpn-instance vpn1
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port service-loopback group 1
#
interface Tunnel0 mode gre
 ip binding vpn-instance vpn1
 ip address 20.1.1.1 255.255.255.0
 source Vlan-interface101
 tunnel vpn-instance vpn1
 destination 200.1.1.2
#
bgp 65410
 peer 20.1.1.2 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
  peer 20.1.1.2 enable
#
 ip route-static vpn-instance vpn1 172.2.0.0 24 Tunnel0
#
```

- CE 2

```
#
vlan 101
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 101
#
bgp 65410
 peer 101.1.1.1 as-number 100
 #
 address-family ipv4 unicast
  import-route direct
```

```
  peer 101.1.1.1 enable
#
```

Contents

Introduction

This document provides examples for configuring Multicast Network Address Translation (MC-NAT).

MC-NAT uses a controller to issue OpenFlow flow entries and group entries to a device to forward traffic from a source device on the public network to different endpoints on the private network as needed. Before forwarding a packet, the device uses a group entry to modify the IP address, port number, VLAN, and MAC address of the packet to those matching an endpoint on the private network.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network. In this example, the controller is an Open vSwitch (OVS) controller.

This document assumes that you have basic knowledge of MC-NAT.

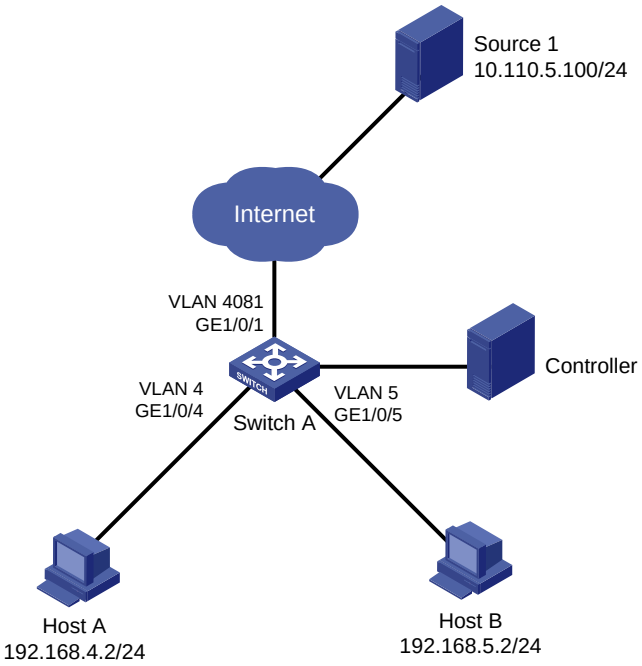
Example: Configuring MC-NAT

Network configuration

As shown in Figure 1, Switch A receives traffic from video source **Source 1** on Internet. Configure the OVS controller to deploy OpenFlow flow entries and group entries to meet the following requirements:

- Switch A translates the public network address to a private network address for a packet received from **Source 1** in VLAN 4081. Switch A sets the destination IP, destination MAC, and destination UDP port number of a packet according to the target host IP.
- Switch A sends the NATed packets to Host A and Host B on the private network.

Figure 1 Network diagram



Device name	MAC	IP	UDP
Source 1	00:02:fc:00:22:2b	11.110.5.100	6457
Host A	00:e0:4c:68:0e:d4	192.168.4.2	4488
Host B	00:50:56:c0:00:08	192.168.5.2	2356

Analysis

- Make sure Switch A and the controller can reach each other so that the OpenFlow instance can establish an OpenFlow channel with the controller. In this example, Switch A uses the management interface to communicate with the controller.
- For the receiver hosts to receive traffic from the source, configure the controller to issue the OpenFlow flow entry and group entry that meet the following requirements:
  - Switch A can use the flow entry to match packets from Source 1.
  - Switch A can use the group entry to change the VLAN ID, destination IP address, destination MAC address, and destination UDP port number of the matching packets to those of Host A and Host B.
  - Switch A can use the group entry to forward the matching packets out of GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported

Hardware	Software version
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported

Hardware	Software version
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring Switch A

Create VLANs. Assign Ethernet interfaces to VLANs as needed.

```
<SwitchA> system-view
[SwitchA] vlan 4 5 4081
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 4081
[SwitchA-GigabitEthernet1/0/1] quit
```

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] port trunk permit vlan 4
[SwitchA-GigabitEthernet1/0/4] quit
[SwitchA] interface gigabitethernet 1/0/5
[SwitchA-GigabitEthernet1/0/5] port link-type trunk
[SwitchA-GigabitEthernet1/0/5] port trunk permit vlan 5
[SwitchA-GigabitEthernet1/0/5] quit
```

Configure M-GigabitEthernet 0/0/0 on Switch A for communicating with the controller.

```
[SwitchA] interface M-GigabitEthernet 0/0/0
[SwitchA-M-GigabitEthernet0/0/0] ip address 172.16.147.136 255.255.0.0
[SwitchA-M-GigabitEthernet0/0/0] quit
```

Create OpenFlow instance 1 and configure it to operate in global mode.

```
[SwitchA] openflow instance 1
[SwitchA-of-inst-1] classification global
```

Specify controller 0 with IP address 172.16.147.101 for OpenFlow instance 1 and activate the instance.

```
[SwitchA-of-inst-1] controller 0 address ip 172.16.147.101
[SwitchA-of-inst-1] active instance
[SwitchA-of-inst-1] quit
```

Configuring the OVS controller

Create group entry 1 that contains the following buckets to OpenFlow instance 1:

- Bucket 1 that contains the following actions:
  - Send the packets out of GigabitEthernet 1/0/4.
  - Change the following fields in the packets: VLAN ID (4), destination IP address (192.168.4.2), destination MAC address (00:e0:4c:68:0e:d4), and destination UDP port number (4488).
- Bucket 2 that contains the following actions:
  - Send the packets out of GigabitEthernet 1/0/5.
  - Change the following fields in the packets: VLAN ID (5), destination IP address (192.168.5.2), destination MAC address (00:50:56:c0:00:08), and destination UDP port number (2356).

```
[root@openflowvm:~/controller0]# ./ovs-appctl send_group_str 'command(add),type(
all),group_id(1),bucket(actions(output(742),set_field(vlan_vid(4+1)),set_field(eth_ds
t(00:e0:4c:68:0e:d4)),set_field(ipv4_dst(192.168.4.2)),set_field(udp_dst(4488)))),buc
ket(actions(output(743),set_field(vlan_vid(5+1)),set_field(eth_dst(00:50:56:c0:00:08)
),set_field(ipv4_dst(192.168.5.2)),set_field(udp_dst(2356))))'
22:46:56|tcp:172.16.147.136:4425: sent (Success): OFPT_GROUP_MOD (xid:31, len:16
0)
22:46:56|OFPT_GROUP_MOD (xid:31)
# Group_Mod
|- command     = add
|- type       = all
|- group_id    = 1
|- bucket
   |- weight      = 0
```

```
   |- watch_port   = any
   |- watch_group  = any
   |- actions
      |- output,742 [max_len = 128]
      |- set_field,vlan_vid,4+1
      |- set_field,eth_dst,00:e0:4c:68:0e:d4
      |- set_field,ipv4_dst,192.168.4.2
      |- set_field,udp_dst,4488
|- bucket
   |- weight      = 0
   |- watch_port   = any
   |- watch_group  = any
   |- actions
      |- output,743 [max_len = 128]
      |- set_field,vlan_vid,5+1
      |- set_field,eth_dst,00:50:56:c0:00:08
      |- set_field,ipv4_dst,192.168.5.2
      |- set_field,udp_dst,2356
[root@openflowvm:~/controller0]#
```

Issue flow entry 1 of table 0 to OpenFlow instance 1. The flow entry contains the following match fields: input port GigabitEthernet 1/0/1, VLAN ID 4081, source IP address 10.110.5.100, source MAC address 00:02:fc:00:22:2b, and source UDP port 6457. Group entry 1 is specified to process the matching packets.

```
[root@openflowvm:~/controller0]# ./ovs-appctl send_flow_str 'command(add),table_
id(0),priority(1),match(in_port(739),vlan_vid(4081+1),eth_src(00:02:fc:00:22:2b),eth_
type(0x800),ipv4_src(10.110.5.100),ip_proto(17),udp_src(6457)),instruction(write_acti
ons(group(1)))'
23:08:24|tcp:172.16.147.136:4425: sent (Success): OFPT_FLOW_MOD (xid:35, len:120
)
23:08:24|OFPT_FLOW_MOD (xid:35)
# Flow_Mod (48)
|- cookie      = 0x0000000000000000
|- cookie_mask  = 0x0000000000000000
|- table_id    = 0
|- command     = add
|- idle_timeout = 0
|- hard_timeout = 0
|- priority    = 1
|- buffer_id   = no_buffer
|- out_port    = any
|- out_group   = any
|- flags       = 0
|- match
   |- in_port,739
   |- vlan_vid,4081+1
   |- eth_src,00:02:fc:00:22:2b
   |- eth_type,0x0800
   |- ipv4_src,10.110.5.100
   |- ip_proto,17
```

```
   |- udp_src,6457
|- instructions
   |- write_actions
      |- group,1
[root@openflowvm:~/controller0]#
```

Verifying the configuration

Verify the configuration on Switch A.

Display group entry information for OpenFlow instance 1 on Switch A.

```
[SwitchA] display openflow instance 1 group
Instance 1 group table information:
 Group count: 1

Group entry 1:
 Type: All, byte count: 0, packet count: 0
 Bucket 1 information:
  Action count 2, watch port: any, watch group: any
  Byte count 0, packet count 0
  Set field:
   Ethernet destination MAC address: 00e0-4c68-0ed4
   VLAN ID: 4
   IPv4 destination address: 192.168.4.2
   UDP destination port: 4488
  Output interface: GE1/0/4
 Bucket 2 information:
  Action count 2, watch port: any, watch group: any
  Byte count 0, packet count 0
  Set field:
   Ethernet destination MAC address: 0050-56c0-0008
   VLAN ID: 5
   IPv4 destination address: 192.168.5.2
   UDP destination port: 2356
  Output interface: GE1/0/5

 Referenced information:
  Count: 1
  Flow table: 0
  Flow entry: 1
```

The output shows that OpenFlow instance 1 has created the group entry issued by the OVS controller. Group entry 1 is configured to set the specified fields in matching packets and send the modified packets out of GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5.

```
[SwitchA] display openflow instance 1 flow
Instance 1 flow table information:

Table 0 information:
 Table type: Extensibility, flow entry count: 1, total flow entry count: 2
```

```
MissRule (default) flow entry information:
 cookie: 0x0, priority: 0, hard time: 0, idle time: 0, flags: reset_counts,
 byte count: 383689, packet count: 3330
 Create time:19:07:20 01/06/2019,  Last modified time:19:07:20 01/06/2019
Match information: any
Instruction information:
 Write actions:
  Drop

Flow entry 1 information:
 cookie: 0x0, priority: 1, hard time: 0, idle time: 0, flags: none,
 byte count: 0, packet count: 0
 Create time:19:30:33 01/06/2019,  Last modified time:19:30:33 01/06/2019
Match information:
 Input interface: GE1/0/1
 Ethernet source MAC address: 0002-fc00-222b
 Ethernet source MAC address mask: ffff-ffff-ffff
 Ethernet type: 0x0800
 VLAN ID: 4081, mask: 0xfff
 IP protocol: 17
 IPv4 source address: 10.110.5.100, mask: 255.255.255.255
 UDP source port: 6457, mask: 0xffff
Instruction information:
 Write actions:
  Group: 1
```

The output shows that OpenFlow instance 1 has created the flow entry issued by the OVS controller in table 0. The instance will use the flow entry to match packets from Source 1 and use group entry 1 to process the matching packets.

Configuration files

- Switch A:

```
#
interface M-GigabitEthernet0/0/0
 ip address 172.16.147.136 255.255.0.0
#
openflow instance 1
 classification global
 controller 0 address ip 172.16.147.101
 active instance
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 4081
#
interface GigabitEthernet1/0/4
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 1 4
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 5
#
```

Contents

Introduction

The following information provides M-LAG configuration examples.

M-LAG is a cross-device link aggregation technology. It aggregates two physical devices on the aggregation layer into one device to provide device-level redundancy protection and load sharing.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of M-LAG.

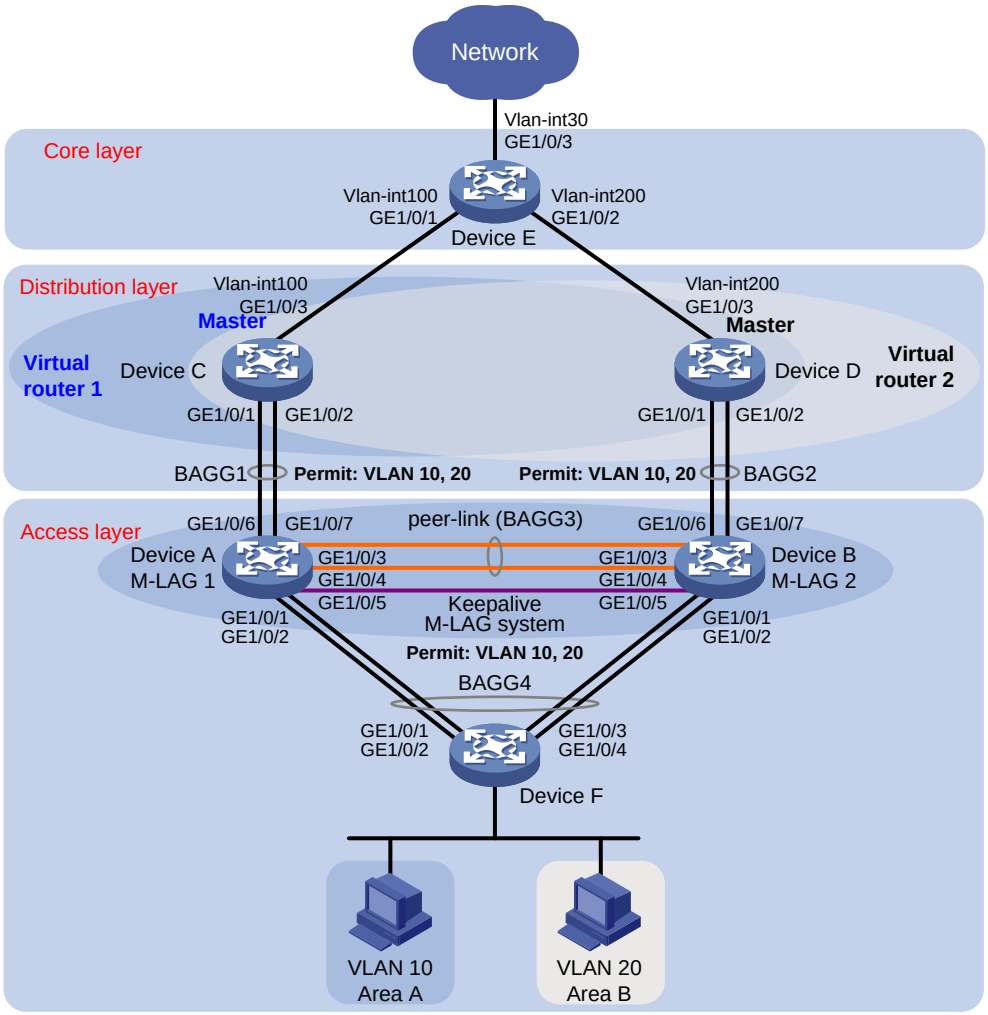
Example: Configuring access-layer M-LAG

Network configuration

As shown in Figure 1, Device A and Device B are access devices, while Device C and Device D act as gateways. Use the M-LAG technology to implement redundancy protection and traffic load sharing for access devices. The specific requirements are as follows:

- Deploy M-LAG on Device A and Device B to achieve redundancy backup and load sharing for access devices.
- Exclude the interface used for M-LAG keepalive detection from the shutdown action by M-LAG MAD on Device A and Device B to detect faults on Device A and Device B.
- Deploy VRRP on Device C and Device D. When the gateways are operating normally, users in area A use gateway Device C for data forwarding while the users in area B use gateway Device D for data forwarding to achieving traffic load sharing.
- When Device C or its uplink interface fails, Device D can quickly take over the task of forwarding host traffic in area A. After Device C recovers from the failure, it resumes its role as the gateway for VRRP group 1.
- When Device D or its uplink interface fails, Device C can quickly take over the task of forwarding host traffic in area B. After Device D recovers from the failure, it resumes its role as the gateway for VRRP group 2.
- Set up an OSPF network on Device C, Device D, and Device E. Use OSPF on Device C and Device D to advertise routes for the subnets where hosts in areas A and B are located. This configuration enables Layer 3 communication between hosts in areas A and B and the external network.

Figure 1 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	GE 1/0/5	1.1.1.1/24	Device B	GE 1/0/5	1.1.1.2/24
Device C	Vlan-int100	100.1.1.1/24	Device D	Vlan-int200	200.1.1.1/24
	Vlan-int10	10.1.1.1/24		Vlan-int10	10.1.1.2/24
	Vlan-int20	20.1.1.1/24		Vlan-int20	20.1.1.2/24
	Virtual IP 1	10.1.1.100/24		Virtual IP 1	10.1.1.100/24
	Virtual IP 2	20.1.1.100/24		Virtual IP 2	20.1.1.100/24
Device E	Vlan-int100	100.1.1.2/24			
	Vlan-int200	200.1.1.2/24			
	Vlan-int30	30.1.1.1/24			

Analysis

- Assign IP addresses to the interfaces used for M-LAG keepalive detection excluded from the shutdown action by M-LAG MAD on Device A and Device B. Make sure the interfaces can communicate at Layer 3.

- To make Device C and Device D become the master devices of VRRP groups 1 and 2, respectively, configure a higher priority for Device C in VRRP group 1 and a higher priority for Device D in VRRP group 2.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported

Hardware	Software version
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When configuring M-LAG, follow these restrictions and guidelines:

- Make sure all M-LAG member devices have the same system MAC address and priority but different system numbers.
- Only one peer link can be configured on an M-LAG device.
- As a best practice, exclude the keepalive interface from the shutdown action by M-LAG MAD to prevent it from being set to the MAD DOWN state during the M-LAG setup process, which could lead to detection errors.

When configuring VRRP, follow these restrictions and guidelines:

- The virtual IP address of a VRRP group cannot be 0.0.0.0, 255.255.255.255, loopback address, non-class-A/B/C address, or other illegal IP addresses such as 0.0.0.1.
- As a best practice, configure the virtual IP address of a VRRP group and the IP addresses of the group member devices' downlink interfaces to be in the same subnet. If you cannot do that, hosts in the LAN might fail to access the external network.

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **reserve-vlan-interface** command to reserve local VLAN interface resources. For more information about the **reserve-vlan-interface** command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure the M-LAG system parameters.

```
<DeviceA> system-view
[DeviceA] m-lag system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceA] m-lag system-number 1
Changing the system number might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceA] m-lag system-priority 123
Changing the system priority might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceA] m-lag keepalive ip destination 1.1.1.2 source 1.1.1.1
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface used for M-LAG keepalive detection from the shutdown action by MAD.

```
[DeviceA] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create VLAN 10 and VLAN 20.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 20
[DeviceA-vlan20] quit
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/6 and GigabitEthernet 1/0/7 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/6] quit
[DeviceA] interface gigabitethernet 1/0/7
[DeviceA-GigabitEthernet1/0/7] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/7] quit
```

Set the link type of Bridge-Aggregation 1 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceA-Bridge-Aggregation1] quit
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 3.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 3 as the peer link interface.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port m-lag peer-link 1
[DeviceA-Bridge-Aggregation3] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 4, and configure it as M-LAG interface 4.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation4] port m-lag group 4
[DeviceA-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 4.

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 4
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 4
[DeviceA-GigabitEthernet1/0/2] quit
```

Set the link type of Bridge-Aggregation 4 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceA] interface bridge-aggregation 4
[DeviceA-Bridge-Aggregation4] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation4] quit
```

Configuring Device B

Configure the M-LAG system parameters.

```
<DeviceB> system-view
[DeviceB] m-lag system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceB] m-lag system-number 2
Changing the system number might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceB] m-lag system-priority 123
Changing the system priority might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceB] m-lag keepalive ip destination 1.1.1.1 source 1.1.1.2
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for M-LAG keepalive detection from the shutdown action by MAD.

```
[DeviceB] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create VLAN 10 and VLAN 20.

```
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 2.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/6 and GigabitEthernet 1/0/7 to aggregation group 2.

```
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/6] quit
[DeviceB] interface gigabitethernet 1/0/7
[DeviceB-GigabitEthernet1/0/7] port link-aggregation group 2
[DeviceB-GigabitEthernet1/0/7] quit
```

Set the link type of Bridge-Aggregation 2 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] port link-type trunk
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceB-Bridge-Aggregation2] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/6 done.
Configuring GigabitEthernet1/0/7 done.
[DeviceB-Bridge-Aggregation2] quit
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 3.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 3 as the peer link interface.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port m-lag peer-link 1
[DeviceB-Bridge-Aggregation3] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 4, and configure it as M-LAG interface 4.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation4] port m-lag group 4
[DeviceB-Bridge-Aggregation4] quit
```

Assign GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to aggregation group 4.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 4
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 4
[DeviceB-GigabitEthernet1/0/2] quit
```

Set the link type of Bridge-Aggregation 4 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceB] interface bridge-aggregation 4
[DeviceB-Bridge-Aggregation4] port link-type trunk
```

```
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation4] quit
```

Configuring Device C

Create VLANs 10, 20, and 100.

```
<DeviceC> system-view
[DeviceC] vlan 10
[DeviceC-vlan10] quit
[DeviceC] vlan 20
[DeviceC-vlan20] quit
[DeviceC] vlan 100
```

Assign GigabitEthernet 1/0/3 to VLAN 100.

```
[DeviceC] vlan 100
[DeviceC-vlan100] port gigabitethernet 1/0/3
[DeviceC-vlan100] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 1 and configure the interface to operate in dynamic mode.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 1
[DeviceC-if-range] quit
```

Set the link type of Bridge-Aggregation 1 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation1] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation1] quit
```

Create VLAN-interface 100 as the uplink interface and assign it an IP address.

```
[DeviceC] interface vlan-interface 100
[DeviceC-Vlan-interface100] ip address 100.1.1.1 24
[DeviceC-Vlan-interface100] quit
```

Create VLAN-interface 10 and VLAN-interface 20 and assign them IP addresses.

```
[DeviceC] interface vlan-interface 10
[DeviceC-vlan-interface10] ip address 10.1.1.1 24
[DeviceC-vlan-interface10] quit
[DeviceC] interface vlan-interface 20
```

```
[DeviceC-vlan-interface20] ip address 20.1.1.1 24
[DeviceC-vlan-interface20] quit
```

Create VRRP group 1 on VLAN-interface 1 and set its virtual IP address to 10.1.1.10.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 virtual-ip 10.1.1.100
```

Set the priority of Device C to 200 for it to become the master in VRRP group 1, so it has the same role in the M-LAG system.

```
[DeviceC-Vlan-interface10] vrrp vrid 1 priority 200
[DeviceC-Vlan-interface10] quit
```

Create VRRP group 2 on VLAN-interface 2 and set its virtual IP address to 20.1.1.10.

```
[DeviceC] interface vlan-interface 20
[DeviceC-Vlan-interface20] vrrp vrid 2 virtual-ip 20.1.1.100
[DeviceC-vlan-interface20] quit
```

Configure Device C to operate in preemptive mode in VRRP group 1, and set the preemption delay to 500 centiseconds.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 preempt-mode delay 500
[DeviceC-Vlan-interface10] quit
```

Create track entry 1 associated with uplink interface GigabitEthernet 1/0/3.

```
[DeviceC] track 1 interface gigabitethernet 1/0/3
```

Associate VRRP group 1 with track entry 1 and decrease the router priority of Device C by 150 when the state of track entry 1 changes to Negative.

```
[DeviceC] interface vlan-interface 10
[DeviceC-Vlan-interface10] vrrp vrid 1 track 1 priority reduced 150
[DeviceC-Vlan-interface10] quit
```

Configure OSPF.

```
[DeviceC] ospf
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

Configuring Device D

Create VLANs 10, 20, and 200.

```
<DeviceD> system-view
[DeviceD] vlan 10
[DeviceD-vlan10] quit
[DeviceD] vlan 20
[DeviceD-vlan20] quit
[DeviceD] vlan 200
```

Assign GigabitEthernet 1/0/3 to VLAN 200.

```
[DeviceD] vlan 200
[DeviceD-vlan200] port gigabitethernet 1/0/3
[DeviceD-vlan200] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 2 and set its aggregation mode to dynamic.

```
[DeviceD] interface bridge-aggregation 2
[DeviceD-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation2] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 2.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-aggregation group 2
[DeviceD-if-range] quit
```

Set the link type of Bridge-Aggregation 2 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceD] interface bridge-aggregation 2
[DeviceD-Bridge-Aggregation2] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation2] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation2] quit
```

Create VLAN-interface 200 as the uplink interface and assign it an IP address.

```
[DeviceD] interface vlan-interface 200
[DeviceD-Vlan-interface200] ip address 200.1.1.1 24
[DeviceD-Vlan-interface200] quit
```

Create VLAN-interface 10 and VLAN-interface 20 and assign them IP addresses.

```
[DeviceD] interface vlan-interface 10
[DeviceD-vlan-interface10] ip address 10.1.1.2 24
[DeviceD-vlan-interface10] quit
[DeviceD] interface vlan-interface 20
[DeviceD-vlan-interface20] ip address 20.1.1.2 24
[DeviceD-vlan-interface20] quit
```

Create VRRP group 1 on VLAN-interface 10 and set its virtual IP address to 10.1.1.100.

```
[DeviceD] interface vlan-interface 10
[DeviceD-Vlan-interface10] vrrp vrid 1 virtual-ip 10.1.1.100
[DeviceD-vlan-interface10] quit
```

Create VRRP group 20 on VLAN-interface 2 and set its virtual IP address to 20.1.1.100.

```
[DeviceD] interface vlan-interface 20
[DeviceD-Vlan-interface20] vrrp vrid 2 virtual-ip 20.1.1.100
```

Set the priority of Device D to 200 for it to become the master in VRRP group 2, so it has the same role in the M-LAG system.

```
[DeviceD-Vlan-interface20] vrrp vrid 2 priority 200
```

Configure Device D to operate in preemptive mode in VRRP group 2, and set the preemption delay to 500 centiseconds.

```
[DeviceD-Vlan-interface20] vrrp vrid 2 preempt-mode delay 500
[DeviceD-Vlan-interface20] quit
```

Create track entry 2 associated with uplink interface GigabitEthernet 1/0/3.

```
[DeviceD] track 2 interface gigabitethernet 1/0/3
```

Associate VRRP group 2 with track entry 2 and decrease the router priority of Device D by 150 when the state of track entry 2 changes to Negative.

```
[DeviceD] interface vlan-interface 20
[DeviceD-Vlan-interface20] vrrp vrid 2 track 2 priority reduced 150
[DeviceD-Vlan-interface20] quit
```

Configure OSPF.

```
[DeviceD] ospf
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Configuring Device E

Create VLAN 100. Assign GigabitEthernet 1/0/1 to the VLAN.

```
<DeviceE> system-view
[DeviceE] vlan 100
[DeviceE-vlan100] port gigabitethernet 1/0/1
[DeviceE-vlan100] quit
```

Create VLAN-interface 100 and assign it an IP address.

```
[DeviceE] interface vlan-interface 100
[DeviceE-vlan-interface100] ip address 100.1.1.2 24
[DeviceE-vlan-interface100] quit
```

Create VLAN 200. Assign GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceE] vlan 200
[DeviceE-vlan200] port gigabitethernet 1/0/2
[DeviceE-vlan200] quit
```

Create VLAN-interface 200 and assign it an IP address.

```
[DeviceE] interface vlan-interface 200
[DeviceE-vlan-interface200] ip address 200.1.1.2 24
[DeviceE-vlan-interface200] quit
```

Create VLAN 30. Assign GigabitEthernet 1/0/3 to the VLAN.

```
[DeviceE] vlan 30
[DeviceE-vlan30] port gigabitethernet 1/0/3
[DeviceE-vlan30] quit
```

Create VLAN-interface 30 and assign it an IP address.

```
[DeviceE] interface vlan-interface 30
[DeviceE-vlan-interface30] ip address 30.1.1.1 24
[DeviceE-vlan-interface30] quit
```

Configure OSPF.

```
[DeviceD] ospf
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

Configuring Device F

Create VLAN 10 and VLAN 20.

```
[DeviceF] vlan 10
[DeviceF-vlan10] quit
[DeviceF] vlan 20
[DeviceF-vlan20] quit
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 4.

```
[DeviceF] interface bridge-aggregation 4
[DeviceF-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceF-Bridge-Aggregation4] quit
```

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to aggregation group 4.

```
[DeviceF] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceF-if-range] port link-aggregation group 4
[DeviceF-if-range] quit
```

Set the link type of Bridge-Aggregation 4 to trunk, and assign it to VLAN 10 and VLAN 20.

```
[DeviceF] interface bridge-aggregation 4
[DeviceF-Bridge-Aggregation4] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceF-Bridge-Aggregation4] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
Configuring GigabitEthernet1/0/3 done.
Configuring GigabitEthernet1/0/4 done.
[DeviceF-Bridge-Aggregation4] quit
```

Verifying the configuration

Display summary information about the peer-link interface and M-LAG interfaces on Device A. Verify that Device A and Device B have successfully formed an M-LAG system.

```
[DeviceA] display m-lag summary
Flags: A -- Aggregate interface down, B -- No peer M-LAG interface configured
       C -- Configuration consistency check failed

Peer-link interface: BAGG3
Peer-link interface state (cause): UP
Keepalive link state (cause): UP

                    M-LAG interface information
M-LAG IF    M-LAG group  Local state (cause)  Peer state  Remaining down time(s)
BAGG4       4            UP                   UP          -
[DeviceA] display m-lag verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- PeerLink_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
```

```
       G -- Port_Sync, H -- Expired

Peer-link interface/Peer-link interface ID: BAGG3/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (2), GE1/0/4 (5)
Peer Selected ports indexes: 2, 5

M-LAG interface/M-LAG group ID: BAGG4/4
Local M-LAG interface state: UP
Peer M-LAG interface state: UP
M-LAG group state: UP
Local M-LAG interface down cause: -
Remaining M-LAG DOWN time: -
Local M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local M-LAG interface LACP priority: Config=32768, Effective=123
Peer M-LAG interface LACP priority: Config=32768, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (16385), GE1/0/2 (16388)
Peer Selected ports indexes: 32769, 32772
```

On Device F, display detailed information about the aggregation groups that correspond to the specified aggregate interfaces. Interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 on Device F are all in Selected state,. In this case, Device F considers Device A and Device B as a single device, thereby achieving cross-device aggregation.

```
[DeviceF] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation4
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 1eba-3c46-0300
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
  GE1/0/3             S        32768    3        1                      {ACDEF}
  GE1/0/4             S        32768    4        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16385    40004    0x7b  , 0001-0001-0001 {ACDEF}
```

```
  GE1/0/2             32768    16388    40004    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/3             32768    32769    40004    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/4             32768    32772    40004    0x7b  , 0001-0001-0001 {ACDEF}
```

Display VRRP group information on Device C and Device D. Device C is the master device in VRRP group 1, and Device D is the master device in VRRP group 2, ensuring that hosts in area A communicate externally through Device C and hosts in area B communicate externally through Device D.

```
[DeviceC] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan10             1     Master       200     100     None     10.1.1.100
 Vlan20             2     Backup       100     100     None     20.1.1.100
[DeviceD] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                       Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan10             1     Backup       100     100     None     10.1.1.100
 Vlan20             2     Master       200     100     None     20.1.1.100
```

Display the OSPF neighbor information of Device E. The output shows that Device E has established neighbors with Device C and Device D to ensure Layer 3 connectivity.

```
[DeviceE] display ospf peer

         OSPF Process 1 with Router ID 200.1.1.2
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 100.1.1.1       100.1.1.1       1   35         Full/BDR          Vlan100
 200.1.1.1       200.1.1.1       1   33         Full/BDR          Vlan200
```

Verify that you can successfully ping 30.1.1.1 on a host in area A.

```
C:\Documents and Settings\Administrator>ping 30.1.1.1

Pinging 30.1.1.1 with 32 bytes of data:

Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 30.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Configuration files

- Device A:

```
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
 port m-lag group 4
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
```

```
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 3
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
 m-lag system-mac 0001-0001-0001
 m-lag system-number 1
 m-lag system-priority 123
 m-lag keepalive ip destination 1.1.1.2 source 1.1.1.1
#
 m-lag mad exclude interface GigabitEthernet1/0/5
#
```

- Device B:

```
#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
```

```
 port m-lag group 4
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 3
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
 m-lag system-mac 0001-0001-0001
 m-lag system-number 2
 m-lag system-priority 123
 m-lag keepalive ip destination 1.1.1.1 source 1.1.1.2
#
 m-lag mad exclude interface GigabitEthernet1/0/5
```

```
#
```

- Device C:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 100
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.100
 vrrp vrid 1 priority 200
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 150
#
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
 vrrp vrid 2 virtual-ip 20.1.1.100
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode bridge
```

```
 port access vlan 100
#
 track 1 interface GigabitEthernet1/0/3
#
```

- Device D:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 200
#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.100
#
interface Vlan-interface20
 ip address 20.1.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 20.1.1.100
 vrrp vrid 2 priority 200
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 2 priority reduced 150
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 2
```

```
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 200
#
 track 2 interface GigabitEthernet1/0/3
#
```

- Device E:

```
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 200.1.1.0 0.0.0.255
#
vlan 30
#
vlan 100
#
vlan 200
#
interface Vlan-interface30
 ip address 30.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 200.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
```

- Device F:

```
#
vlan 10
#
vlan 20
#
```

```
interface Bridge-Aggregation4
 port link-type trunk
 port trunk permit vlan 1 10 20
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 20
 port link-aggregation group 4
#
```

Example: Configuring distribution-layer M-LAG

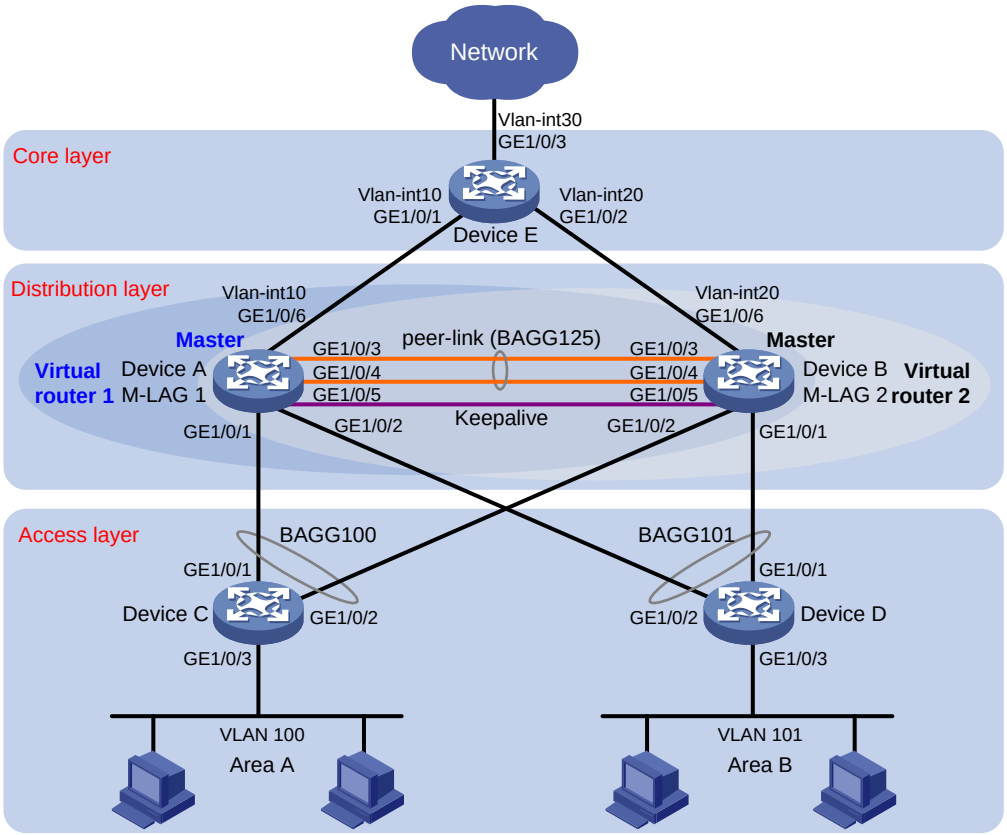
Network configuration

As shown in Figure 2, Device A and Device B are distribution layer devices. Deploy M-LAG and VRRP on Device A and Device B to meet the following requirements:

- When a link on Device A fails, traffic can quickly switch to the link on Device B to ensure reliability. To efficiently utilize bandwidth, Device A and Device B can simultaneously forward packets through their links to achieve load sharing.
- When the gateways are operating normally, users in area A use gateway Device A for data forwarding while the users in area B use gateway Device B for data forwarding to achieving traffic load sharing.
- When Device A or its uplink interface fails, Device B can quickly take over the task of forwarding host traffic in area A. After Device A recovers from the failure, it resumes its role as the gateway for VRRP group 1.

- When Device B or its uplink interface fails, Device A can quickly take over the task of forwarding host traffic in area B. After Device B recovers from the failure, it resumes its role as the gateway for VRRP group 2.
- Set up an OSPF network on Device A, Device B, and Device E. Use OSPF on Device A and Device B to advertise routes for the subnets where hosts in areas A and B are located. This configuration enables Layer 3 communication between hosts in areas A and B and the external network.

Figure 2 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	GE 1/0/5	1.1.1.1/24	Device B	GE 1/0/5	1.1.1.2/24
	Vlan-int100	100.1.1.1/24		Vlan-int100	100.1.1.2/24
	Vlan-int101	101.1.1.1/24		Vlan-int101	101.1.1.2/24
	Vlan-int10	10.1.1.1/24		Vlan-int20	20.1.1.1/24
	Virtual IP 1	100.1.1.100/24		Virtual IP 1	100.1.1.100/24
	Virtual IP 2	101.1.1.100/24		Virtual IP 2	101.1.1.100/24
Device E	Vlan-int10	10.1.1.2/24			
	Vlan-int20	20.1.1.2/24			
	Vlan-int30	30.1.1.1/24			

Analysis

- Assign IP addresses to the interfaces used for M-LAG keepalive detection excluded from the shutdown action by M-LAG MAD on Device A and Device B. Make sure the interfaces can communicate at Layer 3.

- To make Device A and B become the master devices of VRRP groups 1 and 2, respectively, configure a higher priority for Device A in VRRP group 1 and a higher priority for Device B in VRRP group 2.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported

Hardware	Software version
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

When configuring M-LAG, follow these restrictions and guidelines:

- Make sure all M-LAG member devices have the same system MAC address and priority but different system numbers.
- Only one peer link can be configured on an M-LAG device.
- As a best practice, exclude the keepalive interface from the shutdown action by M-LAG MAD to prevent it from being set to the MAD DOWN state during the M-LAG setup process, which could lead to detection errors.

When configuring VRRP, follow these restrictions and guidelines:

- The virtual IP address of a VRRP group cannot be 0.0.0.0, 255.255.255.255, loopback address, non-class-A/B/C address, or other illegal IP addresses such as 0.0.0.1.
- As a best practice, configure the virtual IP address of a VRRP group and the IP addresses of the group member devices' downlink interfaces to be in the same subnet. If you cannot do that, hosts in the LAN might fail to access the external network.

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **reserve-vlan-interface** command to reserve local VLAN interface resources. For more information about the reserve-vlan-interface command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure the M-LAG system parameters.

```
<DeviceA> system-view
[DeviceA] m-lag system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceA] m-lag system-number 1
Changing the system number might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceA] m-lag system-priority 123
Changing the system priority might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceA] m-lag keepalive ip destination 1.1.1.2 source 1.1.1.1
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 1.1.1.1 24
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface used for M-LAG keepalive detection from the shutdown action by MAD.

```
[DeviceA] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 125.

```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation125] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 125.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 125 as the peer link interface.

```
[DeviceA] interface bridge-aggregation 125
[DeviceA-Bridge-Aggregation125] port m-lag peer-link 1
[DeviceA-Bridge-Aggregation125] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 100, and configure it as M-LAG interface 1.

```
[DeviceA] interface bridge-aggregation 100
[DeviceA-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation100] port m-lag group 1
[DeviceA-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 100.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 100
[DeviceA-GigabitEthernet1/0/1] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 101, and configure it as M-LAG interface 2.

```
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation101] port m-lag group 2
[DeviceA-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 101
[DeviceA-GigabitEthernet1/0/2] quit
```

Create VLANs 10, 100, and 101.

```
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit
```

Assign GigabitEthernet 1/0/6 to VLAN 10.

```
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/6
[DeviceA-vlan10] quit
```

Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceA] interface bridge-aggregation 100
```

```
[DeviceA-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
[DeviceA-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/1 done.
[DeviceA-Bridge-Aggregation100] quit
```

Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceA] interface bridge-aggregation 101
[DeviceA-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/2 done.
[DeviceA-Bridge-Aggregation101] quit
```

Create VLAN-interface 10, VLAN-interface 20, and VLAN-interface 101 and assign them IP addresses.

```
[DeviceA] interface vlan-interface 10
[DeviceA-vlan-interface10] ip address 10.1.1.1 24
[DeviceA-vlan-interface10] quit
[DeviceA] interface vlan-interface 100
[DeviceA-vlan-interface100] ip address 100.1.1.1 24
[DeviceA-vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-vlan-interface101] ip address 101.1.1.1 24
[DeviceA-vlan-interface101] quit
```

Configure OSPF.

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 101.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 100.1.1.100.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 virtual-ip 100.1.1.100
```

Set the priority of Device A to 200 for it to become the master in VRRP group 1, so it has the same role in the M-LAG system.

```
[DeviceA-Vlan-interface100] vrrp vrid 1 priority 200
[DeviceA-Vlan-interface100] quit
```

Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 101.1.1.100.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] vrrp vrid 2 virtual-ip 101.1.1.100
[DeviceA-Vlan-interface101] quit
```

Configure Device A to operate in preemptive mode in VRRP group 1, and set the preemption delay to 500 centiseconds.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 preempt-mode delay 500
[DeviceA-Vlan-interface100] quit
```

Create track entry 1 associated with uplink interface GigabitEthernet 1/0/6.

```
[DeviceA] track 1 interface gigabitethernet 1/0/6
```

Associate VRRP group 1 with track entry 1 and decrease the router priority of Device A by 150 when the state of track entry 1 changes to Negative.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] vrrp vrid 1 track 1 priority reduced 150
[DeviceA-Vlan-interface100] quit
```

Configuring Device B

Configure the M-LAG system parameters.

```
<DeviceB> system-view
[DeviceB] m-lag system-mac 1-1-1
Changing the system MAC might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceB] m-lag system-number 2
Changing the system number might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
[DeviceB] m-lag system-priority 123
Changing the system priority might flap the intra-portal link and cause M-LAG system setup
failure. Continue? [Y/N]:y
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceB] m-lag keepalive ip destination 1.1.1.1 source 1.1.1.2
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 1.1.1.2 24
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for M-LAG keepalive detection from the shutdown action by MAD.

```
[DeviceB] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 125.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation125] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 125.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 125
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 125
[DeviceB-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 125 as the peer link interface.

```
[DeviceB] interface bridge-aggregation 125
[DeviceB-Bridge-Aggregation125] port m-lag peer-link 1
[DeviceB-Bridge-Aggregation125] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 100, and configure it as M-LAG interface 1.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation100] port m-lag group 1
[DeviceB-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/2 to aggregation group 100.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 100
[DeviceB-GigabitEthernet1/0/2] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 101, and configure it as M-LAG interface 2.

```
[DeviceB] interface bridge-aggregation 101
[DeviceB-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation101] port m-lag group 2
[DeviceB-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 101.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 101
[DeviceB-GigabitEthernet1/0/1] quit
```

Create VLANs 20, 100, and 101.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] vlan 101
[DeviceB-vlan101] quit
```

Assign GigabitEthernet 1/0/6 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/6
[DeviceB-vlan20] quit
```

Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceB] interface bridge-aggregation 100
[DeviceB-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/2 done.
[DeviceB-Bridge-Aggregation100] quit
```

Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceB] interface bridge-aggregation 101
[DeviceB-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
[DeviceB-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/1 done.
[DeviceB-Bridge-Aggregation101] quit
```

Create VLAN-interface 20, VLAN-interface 100, and VLAN-interface 101 and assign them IP addresses.

```
[DeviceB] interface vlan-interface 20
[DeviceB-vlan-interface20] ip address 20.1.1.1 24
[DeviceB-vlan-interface20] quit
[DeviceB] interface vlan-interface 100
[DeviceB-vlan-interface100] ip address 100.1.1.2 24
[DeviceB-vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ip address 101.1.1.2 24
[DeviceB-vlan-interface101] quit
```

Configure OSPF.

```
[DeviceB] ospf
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 100.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 101.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

Create VRRP group 1 on VLAN-interface 100 and set its virtual IP address to 100.1.1.100.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] vrrp vrid 1 virtual-ip 100.1.1.100
[DeviceB-Vlan-interface100] quit
```

Create VRRP group 2 on VLAN-interface 101 and set its virtual IP address to 101.1.1.100.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 2 virtual-ip 101.1.1.100
```

Set the priority of Device B to 200 for it to become the master in VRRP group 2, so it has the same role in the M-LAG system.

```
[DeviceA-Vlan-interface101] vrrp vrid 2 priority 200
```

Configure Device B to operate in preemptive mode in VRRP group 2, and set the preemption delay to 500 centiseconds.

```
[DeviceB-Vlan-interface101] vrrp vrid 2 preempt-mode delay 500
[DeviceB-Vlan-interface101] quit
```

Create track entry 2 associated with uplink interface GigabitEthernet 1/0/6.

```
[DeviceB] track 2 interface gigabitethernet 1/0/6
```

Associate VRRP group 2 with track entry 2 and decrease the router priority of Device B by 150 when the state of track entry 2 changes to Negative.

```
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] vrrp vrid 2 track 2 priority reduced 150
[DeviceB-Vlan-interface101] quit
```

Configuring Device C

Create VLAN 100.

```
[DeviceC] vlan 100
[DeviceC-vlan100] quit
```

Assign GigabitEthernet 1/0/3 to VLAN 100.

```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port access vlan 100
```

```
[DeviceC-GigabitEthernet1/0/3] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 100 and configure the interface to operate in dynamic mode.

```
<DeviceC> system-view
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation100] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 100.

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 100
[DeviceC-if-range] quit
```

Set the link type of Bridge-Aggregation 100 to trunk, and assign it to VLAN 100.

```
[DeviceC] interface bridge-aggregation 100
[DeviceC-Bridge-Aggregation100] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation100] port trunk permit vlan 100
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceC-Bridge-Aggregation100] quit
```

Configuring Device D

Create VLAN 101.

```
[DeviceD] vlan 101
[DeviceD-vlan101] quit
```

Assign GigabitEthernet 1/0/3 to VLAN 101.

```
[DeviceD] interface gigabitethernet 1/0/3
[DeviceD-GigabitEthernet1/0/3] port access vlan 101
[DeviceD-GigabitEthernet1/0/3] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 101 and configure the interface to operate in dynamic mode.

```
<DeviceD> system-view
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation101] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 101.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-aggregation group 101
[DeviceD-if-range] quit
```

Set the link type of Bridge-Aggregation 101 to trunk, and assign it to VLAN 101.

```
[DeviceD] interface bridge-aggregation 101
[DeviceD-Bridge-Aggregation101] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation101] port trunk permit vlan 101
Configuring GigabitEthernet1/0/1 done.
```

```
Configuring GigabitEthernet1/0/2 done.
[DeviceD-Bridge-Aggregation101] quit
```

Configuring Device E

Create VLAN 10. Assign GigabitEthernet 1/0/1 to the VLAN.

```
<DeviceE> system-view
[DeviceE] vlan 10
[DeviceE-vlan10] port gigabitethernet 1/0/1
[DeviceE-vlan10] quit
```

Create VLAN-interface 10 and assign it an IP address.

```
[DeviceE] interface vlan-interface 10
[DeviceE-vlan-interface10] ip address 10.1.1.2 24
[DeviceE-vlan-interface10] quit
```

Create VLAN 20. Assign GigabitEthernet 1/0/2 to the VLAN.

```
[DeviceE] vlan 20
[DeviceE-vlan20] port gigabitethernet 1/0/2
[DeviceE-vlan20] quit
```

Create VLAN-interface 20 and assign it an IP address.

```
[DeviceE] interface vlan-interface 20
[DeviceE-vlan-interface20] ip address 20.1.1.2 24
[DeviceE-vlan-interface20] quit
```

Create VLAN 30. Assign GigabitEthernet 1/0/3 to the VLAN.

```
[DeviceE] vlan 30
[DeviceE-vlan30] port gigabitethernet 1/0/3
[DeviceE-vlan30] quit
```

Create VLAN-interface 30 and assign it an IP address.

```
[DeviceE] interface vlan-interface 30
[DeviceE-vlan-interface30] ip address 30.1.1.1 24
[DeviceE-vlan-interface30] quit
```

Configure OSPF.

```
[DeviceE] ospf
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

Verifying the configuration

Display summary information about the peer-link interface and M-LAG interfaces on Device A. Verify that Device A and Device B have successfully formed an M-LAG system.

```
[DeviceA] display m-lag summary
Flags: A -- Aggregate interface down, B -- No peer M-LAG interface configured
       C -- Configuration consistency check failed
```

```
Peer-link interface: BAGG125
Peer-link interface state (cause): UP
Keepalive link state (cause): UP

                    M-LAG interface information
M-LAG IF    M-LAG group  Local state (cause)  Peer state  Remaining down time(s)
BAGG100     1            UP                   UP          -
BAGG101     2            UP                   UP          -
[DeviceA] display m-lag verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- PeerLink_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired

Peer-link interface/Peer-link interface ID: BAGG125/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (1), GE1/0/4 (4)
Peer Selected ports indexes: 1, 4

M-LAG interface/M-LAG group ID: BAGG100/1
Local M-LAG interface state: UP
Peer M-LAG interface state: UP
M-LAG group state: UP
Local M-LAG interface down cause: -
Remaining M-LAG DOWN time: -
Local M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local M-LAG interface LACP priority: Config=32768, Effective=123
Peer M-LAG interface LACP priority: Config=32768, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (16386)
Peer Selected ports indexes: 32771

M-LAG interface/M-LAG group ID: BAGG101/2
Local M-LAG interface state: UP
Peer M-LAG interface state: UP
M-LAG group state: UP
Local M-LAG interface down cause: -
Remaining M-LAG DOWN time: -
Local M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Peer M-LAG interface LACP MAC: Config=0001-0001-0001, Effective=0001-0001-0001
Local M-LAG interface LACP priority: Config=32768, Effective=123
Peer M-LAG interface LACP priority: Config=32768, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/2 (16387)
Peer Selected ports indexes: 32772
```

On Device C and Device D, display the detailed information for Layer 2 aggregation group 100 and Layer 2 aggregation group 101, separately. Interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on Device C and Device D are all in Selected state. In this case, Device C and Device D consider Device A and Device B as a single device, thereby achieving cross-device aggregation.

```
[DeviceC] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation100
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 8e33-8e4a-0300
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16386    40001    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    32770    40001    0x7b  , 0001-0001-0001 {ACDEF}
[DeviceD] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation101
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 8e33-9400-0400
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  GE1/0/1             S        32768    1        1                      {ACDEF}
  GE1/0/2             S        32768    2        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)          32768    16387    40002    0x7b  , 0001-0001-0001 {ACDEF}
  GE1/0/2             32768    32771    40002    0x7b  , 0001-0001-0001 {ACDEF}
```

Display VRRP group information on Device A and Device B. Device A is the master device in VRRP group 1, and Device B is the master device in VRRP group 2, ensuring that hosts in area A communicate externally through Device A and hosts in area B communicate externally through Device B.

```
[DeviceA] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan100            1     Master       200     100     None     100.1.1.100
 Vlan101            2     Backup       100     100     None     101.1.1.100
[DeviceB] display vrrp
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 2
 Interface          VRID  State        Running Adver   Auth     Virtual
                                        Pri     Timer   Type        IP
 ------------------------------------------------------------------------
 Vlan100            1     Backup       100     100     None     100.1.1.100
 Vlan101            2     Master       200     100     None     101.1.1.100
```

Display the OSPF neighbor information of Device E. The output shows that Device E has established neighbors with Device A and Device B to ensure Layer 3 connectivity.

```
[DeviceE] display ospf peer

         OSPF Process 1 with Router ID 30.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 101.1.1.1       10.1.1.1        1   34         Full/DR           Vlan10
 101.1.1.2       20.1.1.1        1   36         Full/DR           Vlan20
```

Use the **ping** command on a host in area A to verify that it can successfully ping a host in area B (the host runs Windows XP). This shows that hosts in both area A and area B can ping each other. Verify that a host in area A can successfully ping 30.1.1.1. The preceding information indicates that Layer 3 forwarding is achieved through M-LAG.

```
C:\Documents and Settings\Administrator>ping 101.1.1.4

Pinging 101.1.1.4 with 32 bytes of data:

Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126
Reply from 101.1.1.4: bytes=32 time=1ms TTL=126

Ping statistics for 101.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 30.1.1.1

Pinging 30.1.1.1 with 32 bytes of data:

Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126
Reply from 30.1.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 30.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Configuration files

- Device A:

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 101.1.1.0 0.0.0.255
#
vlan 10
#
vlan 100 to 101
#
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
 port m-lag group 1
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
 port m-lag group 2
#
interface Bridge-Aggregation125
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
```

```
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 100.1.1.100
 vrrp vrid 1 priority 200
 vrrp vrid 1 preempt-mode delay 500
 vrrp vrid 1 track 1 priority reduced 150
#
interface Vlan-interface101
 ip address 101.1.1.1 255.255.255.0
 vrrp vrid 2 virtual-ip 101.1.1.100
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 125
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 125
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 10
#
 m-lag system-mac 0001-0001-0001
 m-lag system-number 1
```

```
 m-lag system-priority 123
 m-lag keepalive ip destination 1.1.1.2 source 1.1.1.1
#
 m-lag mad exclude interface GigabitEthernet1/0/5
#
 track 1 interface GigabitEthernet1/0/6
#
```

- Device B:

```
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
  network 101.1.1.0 0.0.0.255
#
vlan 20
#
vlan 100 to 101
#
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
 port m-lag group 1
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
 port m-lag group 2
#
interface Bridge-Aggregation125
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
interface Vlan-interface20
 ip address 20.1.1.1 255.255.255.0
#
interface Vlan-interface100
 ip address 100.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 100.1.1.100
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
 vrrp vrid 2 virtual-ip 101.1.1.100
 vrrp vrid 2 priority 200
```

```
 vrrp vrid 2 preempt-mode delay 500
 vrrp vrid 2 track 2 priority reduced 150
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 125
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 125
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 20
#
 m-lag system-mac 0001-0001-0001
 m-lag system-number 2
 m-lag system-priority 123
 m-lag keepalive ip destination 1.1.1.1 source 1.1.1.2
#
 m-lag mad exclude interface GigabitEthernet1/0/5
#
 track 2 interface GigabitEthernet1/0/6
#
```

- Device C:

```
#
vlan 100
#
```

```
interface Bridge-Aggregation100
 port link-type trunk
 port trunk permit vlan 1 100
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 port link-aggregation group 100
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 100
#
```

- Device D:

```
#
vlan 101
#
interface Bridge-Aggregation101
 port link-type trunk
 port trunk permit vlan 1 101
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 101
 port link-aggregation group 101
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 101
#
```

- Device E:

```
#
```

```
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
vlan 10
#
vlan 20
#
vlan 30
#
interface Vlan-interface10
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface20
 ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface30
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 30
#
```

Example: Configuring IPv4 and IPv6 dual-active VLAN gateways on an M-LAG network

Network configuration

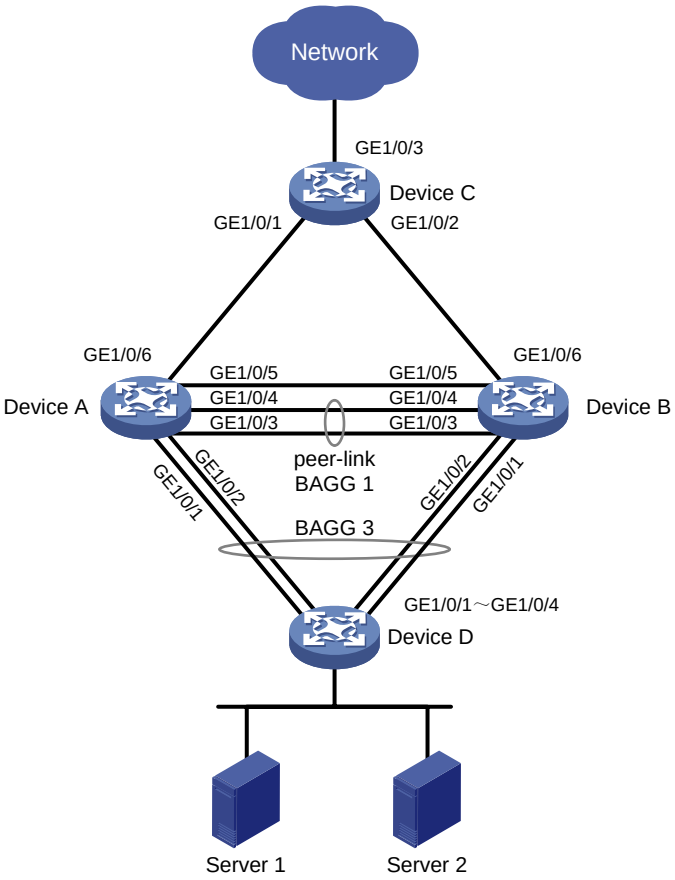
As shown in Figure 3:

- Device A and Device B form an M-LAG system. Device D accesses the M-LAG system through M-LAG interfaces.
- Device A and Device B are connected to uplink device Device C through equal-cost routes.

Configure the network as follows to meet the server access requirements of users:

- The two M-LAG member devices Device A and Device B both act as the IPv4 gateway and IPv6 gateway for the servers.
- If the link between Device A or Device B and uplink device Device C fails, packets can be transmitted along the other M-LAG member device to Device C to avoid interrupting the servers' communication with the external network.

Figure 3 Network diagram



Device	Interface	IP address	Peer device and interface
Device A	GE 1/0/1	-	Device D: GE 1/0/1
	GE 1/0/2	-	Device D: GE 1/0/2
	GE 1/0/3	-	Device B: GE 1/0/3
	GE 1/0/4	-	Device B: GE 1/0/4
	GE 1/0/5	IPv4: 21.1.1.1 IPv6: 21::1	Device B: GE 1/0/5
	GE 1/0/6	-	Device C: GE 1/0/1
	Vlan-int100	IPv4: 100.1.1.100/24 IPv6: 100::100/64	-
	Vlan-int101	IPv4: 101.1.1.1/24 IPv6: 101::1/64	Device B: Vlan-int101 • IPv4: 101.1.1.2/24 • IPv6: 101::2/64

Device	Interface	IP address	Peer device and interface
	Vlan-int32	IPv4: 32.1.1.1/24 IPv6: 32::1/64	Device C: Vlan-int32 • IPv4: 32.1.1.2/24 • IPv6: 32::2/64
Device B	GE 1/0/1	-	Device D: GE 1/0/3
	GE 1/0/2	-	Device D: GE 1/0/4
	GE 1/0/3	-	Device A: GE 1/0/3
	GE 1/0/4	-	Device A: GE 1/0/4
	GE 1/0/5	IPv4: 21.1.1.2 IPv6: 21::2	Device A: GE 1/0/5
	GE 1/0/6	-	Device C: GE 1/0/6
	Vlan-int100	IPv4: 100.1.1.100/24 IPv6: 100::100/64	-
	Vlan-int101	IPv4: 101.1.1.2/24 IPv6: 101::2/64	Device A: Vlan-int101 • IPv4: 101.1.1.1/24 • IPv6: 101::1/64
	Vlan-int33	IPv4: 33.1.1.1/24 IPv6: 33::1/64	Device C: Vlan-int33 • IPv4: 33.1.1.2/24 • IPv6: 33::2/64
Device C	GE 1/0/1	-	Device A: GE 1/0/6
	GE 1/0/2	-	Device B: GE 1/0/6
	GE 1/0/3	-	Network 1
	Vlan-int22	IPv4: 22.1.1.1/24 IPv6: 22::1/64	Network 1
	Vlan-int32	IPv4: 32.1.1.2/24 IPv6: 32::2/64	Device A: Vlan-int32 • IPv4: 32.1.1.1/24 • IPv6: 32::1/64
	Vlan-int33	IPv4: 33.1.1.2/24 IPv6: 33::2/64	Device B: Vlan-int33 • IPv4: 33.1.1.1/24 • IPv6: 33::1/64
Device D	GE 1/0/1	-	Device A: GE 1/0/1
	GE 1/0/2	-	Device A: GE 1/0/2
	GE 1/0/3	-	Device B: GE 1/0/1
	GE 1/0/4	-	Device B: GE 1/0/2

Analysis

- Configure VLAN-interface 100 on Device A and Device B to act as the IPv4 and IPv6 dual-active gateways. To enable IPv4 and IPv6 users to access the external network through the gateways, configure the same IPv4 address, MAC address, IPv6 address, and IPv6 link-local address for VLAN-interface 100 on Device A and Device B.

- Enable Device A and Device B to communicate at Layer 3 through VLAN-interface 101. Then, packets can be routed to the other M-LAG member device when the link between Device A or Device B and uplink device Device C fails.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported

Hardware	Software version
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

The M-LAG system MAC address must be the same for devices in the same M-LAG system. The M-LAG system MAC addresses must be different for devices in different M-LAG systems.

For the S5570S-EI, S5500V3-SI, S3600V3-EI, and S3600V3-SI switch series, before switching a Layer 2 Ethernet interface to a Layer 3 Ethernet interface or creating a Layer 3 aggregate interface, use the **reserve-vlan-interface** command to reserve local VLAN interface resources. For more information about the reserve-vlan-interface command, see the VLAN configuration and VLAN commands for your product.

Procedures

Configuring Device A

Configure the M-LAG system parameters.

```
<DeviceA> system-view
[DeviceA] m-lag system-mac 0002-0002-0002
[DeviceA] m-lag system-number 1
[DeviceA] m-lag system-priority 123
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceA] m-lag keepalive ip destination 21.1.1.2 source 21.1.1.1
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-mode route
[DeviceA-GigabitEthernet1/0/5] ip address 21.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/5] ipv6 address 21::1 64
[DeviceA-GigabitEthernet1/0/5] quit
```

Exclude the interface for the keepalive link from the shutdown action by M-LAG MAD.

```
[DeviceA] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 1.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as the peer link interface.

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port m-lag peer-link 1
[DeviceA-Bridge-Aggregation1] undo port trunk permit vlan 1
[DeviceA-Bridge-Aggregation1] quit
```

Create dynamic Layer 1 dynamic aggregate interface Bridge-Aggregation 3, and configure it as M-LAG interface 2.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] port m-lag group 1
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/2] quit
```

Create VLAN 100 and VLAN 101.

```
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] vlan 101
[DeviceA-vlan101] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port link-type trunk
[DeviceA-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceA-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceA-Bridge-Aggregation3] quit
```

Assign IPv4 address 100.1.1.100 and MAC address 0000-0010-0010 to VLAN-interface 100, which is to act as an IPv4 dual-active gateway.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ip address 100.1.1.100 255.255.255.0
[DeviceA-Vlan-interface100] mac-address 0000-0010-0010
```

Assign IPv6 link-local address 100::100 and MAC address FE80:: 80 to VLAN-interface 100, which is to act as an IPv6 dual-active gateway.

```
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ipv6 address 100::100 64
[DeviceA-Vlan-interface100] ipv6 address FE80::80 link-local
```

Exclude VLAN-interface 100 from the shutdown action by M-LAG MAD.

```
[DeviceA] m-lag mad exclude interface vlan-interface100
```

Create VLAN-interface 101, and assign an IPv4 address and IPv6 address to it, which is used for Layer 3 communication between M-LAG member devices.

```
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ip address 101.1.1.1 255.255.255.0
[DeviceA-Vlan-interface101] ipv6 address 101::1 64
[DeviceA-Vlan-interface101] quit
```

Exclude VLAN-interface 101 from the shutdown action by M-LAG MAD.

```
[DeviceA] m-lag mad exclude interface vlan-interface101
```

Set the router ID to 3.3.3.3.

```
[DeviceA] router id 3.3.3.3
```

Configure OSPF on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPF packets to implement IPv4 connectivity between the M-LAG member devices.

```
[DeviceA] ospf 1
[DeviceA-ospf-1] silent-interface vlan-interface 100
[DeviceA-ospf-1] import-route direct
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ospf 1 area 0.0.0.0
[DeviceA-Vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ospf 1 area 0.0.0.0
[DeviceA-Vlan-interface101] quit
```

Configure OSPFv3 on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPFv3 packets to implement IPv6 connectivity between the M-LAG member devices.

```
[DeviceA] ospfv3 1
[DeviceA-ospfv3-1] silent-interface vlan-interface 100
[DeviceA-ospfv3-1] import-route direct
[DeviceA-ospfv3-1] area 0
[DeviceA-ospfv3-1-area-0.0.0.0] quit
[DeviceA-ospfv3-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] ospfv3 1 area 0.0.0.0
[DeviceA-Vlan-interface100] quit
[DeviceA] interface vlan-interface 101
[DeviceA-Vlan-interface101] ospfv3 1 area 0.0.0.0
[DeviceA-Vlan-interface101] quit
```

Create VLAN 32, and assign the M-LAG uplink interface GigabitEthernet 1/0/6 to VLAN 32.

```
[DeviceA] vlan 32
[DeviceA-vlan32] quit
[DeviceA] interface gigabitethernet 1/0/6
[DeviceA-GigabitEthernet1/0/6] port link-type trunk
[DeviceA-GigabitEthernet1/0/6] port trunk permit vlan 32
[DeviceA-GigabitEthernet1/0/6] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/6] quit
```

Create VLAN-interface 32, assign an IPv4 address and IPv6 address to it, and enable OSPF and OSPFv3 on the interface.

```
[DeviceA] interface vlan-interface 32
[DeviceA-Vlan-interface32] ip address 32.1.1.1 255.255.255.0
[DeviceA-Vlan-interface32] ipv6 address 32::1 64
[DeviceA-Vlan-interface32] ospf 1 area 0
[DeviceA-Vlan-interface32] ospfv3 1 area 0
[DeviceA-Vlan-interface32] quit
```

Configuring Device B

Configure the M-LAG system parameters.

```
<DeviceB> system-view
[DeviceB] m-lag system-mac 0002-0002-0002
[DeviceB] m-lag system-number 2
[DeviceB] m-lag system-priority 123
```

Configure the destination and source IP addresses of keepalive packets.

```
[DeviceB] m-lag keepalive ip destination 21.1.1.1 source 21.1.1.2
```

Set the link mode of GigabitEthernet 1/0/5 to Layer 3, and assign the interface an IP address. The IP address will be used as the source IP address of keepalive packets.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-mode route
[DeviceB-GigabitEthernet1/0/5] ip address 21.1.1.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/5] ipv6 address 21::2 64
[DeviceB-GigabitEthernet1/0/5] quit
```

Exclude the interface used for M-LAG keepalive detection from the shutdown action by MAD.

```
[DeviceB] m-lag mad exclude interface gigabitethernet 1/0/5
```

Create dynamic Layer 2 aggregate interface Bridge-aggregation 1.

```
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 to aggregation group 1.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/3] quit
[DeviceB] interface gigabitethernet 1/0/4
[DeviceB-GigabitEthernet1/0/4] port link-aggregation group 1
[DeviceB-GigabitEthernet1/0/4] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as the peer link interface.

```
[DeviceB] interface bridge-aggregation 1
[DeviceB-Bridge-Aggregation1] port m-lag peer-link 1
[DeviceB-Bridge-Aggregation1] undo port trunk permit vlan 1
[DeviceB-Bridge-Aggregation1] quit
```

Create dynamic Layer 1 dynamic aggregate interface Bridge-Aggregation 3, and configure it as M-LAG interface 2.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] port m-lag group 1
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/2] quit
```

Create VLANs 100 and 101.

```
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] vlan 101
[DeviceB-vlan101] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port link-type trunk
[DeviceB-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceB-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceB-Bridge-Aggregation3] quit
```

Assign IPv4 address 100.1.1.100 and MAC address 0000-0010-0010 to VLAN-interface 100, which is to act as an IPv4 dual-active gateway.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ip address 100.1.1.100 255.255.255.0
[DeviceB-Vlan-interface100] mac-address 0000-0010-0010
```

Assign IPv6 link-local address 100::100 and MAC address FE80:: 80 to VLAN-interface 100, which is to act as an IPv6 dual-active gateway.

```
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ipv6 address 100::100 64
[DeviceB-Vlan-interface100] ipv6 address FE80::80 link-local
```

Exclude VLAN-interface 100 from the shutdown action by M-LAG MAD.

```
[DeviceB] m-lag mad exclude interface vlan-interface100
```

Create VLAN-interface 101, and assign an IPv4 address and IPv6 address to it, which is used for Layer 3 communication between M-LAG member devices.

```
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ip address 101.1.1.2 24
[DeviceB-vlan-interface101] ipv6 address 101::2 64
[DeviceB-vlan-interface101] quit
```

Exclude VLAN-interface 101 from the shutdown action by M-LAG MAD.

```
[DeviceB] m-lag mad exclude interface vlan-interface101
```

Set the router ID to 4.4.4.4.

```
[DeviceB] router id 4.4.4.4
```

Configure OSPF on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPF packets to implement IPv4 connectivity between the M-LAG member devices.

```
[DeviceB] ospf 1
[DeviceB-ospf-1] silent-interface vlan-interface100
[DeviceB-ospf-1] import-route direct
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] ospf 1 area 0.0.0.0
[DeviceB-Vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-Vlan-interface101] ospf 1 area 0.0.0.0
```

```
[DeviceB-Vlan-interface101] quit
```

Configure OSPFv3 on VLAN-interface 100 and VLAN-interface 101. Disable VLAN-interface 100 from receiving and sending OSPFv3 packets to implement IPv6 connectivity between the M-LAG member devices.

```
[DeviceB] ospfv3 1
[DeviceB-ospf-1] silent-interface vlan-interface100
[DeviceB-ospfv3-1] import-route direct
[DeviceB-ospfv3-1] area 0
[DeviceB-ospfv3-1-area-0.0.0.0] quit
[DeviceB-ospfv3-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-vlan-interface100] ospfv3 1 area 0
[DeviceB-vlan-interface100] quit
[DeviceB] interface vlan-interface 101
[DeviceB-vlan-interface101] ospfv3 1 area 0
[DeviceB-vlan-interface101] quit
```

Create VLAN 33, and assign the M-LAG uplink interface GigabitEthernet 1/0/6 to VLAN 33.

```
[DeviceB] vlan 33
[DeviceB-vlan33] quit
[DeviceB] interface gigabitethernet 1/0/6
[DeviceB-GigabitEthernet1/0/6] port link-type trunk
[DeviceB-GigabitEthernet1/0/6] port trunk permit vlan 33
[DeviceB-GigabitEthernet1/0/6] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/6] quit
```

Create VLAN-interface 33, assign an IPv4 address and IPv6 address to it, and enable OSPF and OSPFv3 on the interface.

```
[DeviceB] interface vlan-interface 33
[DeviceB-Vlan-interface33] ip address 33.1.1.1 255.255.255.0
[DeviceB-Vlan-interface33] ipv6 address 33::1 64
[DeviceB-Vlan-interface33] ospf 1 area 0
[DeviceB-Vlan-interface33] ospfv3 1 area 0
[DeviceB-Vlan-interface33] quit
```

Configuring Device C

Create VLAN 32. Assign GigabitEthernet 1/0/1 that connects Device C to Device A to VLAN 32. Assign both an IPv4 address and IPv6 address to VLAN-interface 32.

```
<DeviceC> system-view
[DeviceC] vlan 32
[DeviceC-vlan32] quit
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 32
[DeviceC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ip address 32.1.1.2 24
[DeviceC-Vlan-interface32] ipv6 address 32::2 64
```

```
[DeviceC-Vlan-interface32] quit
```

Create VLAN 33. Assign GigabitEthernet 1/0/2 that connects Device C to Device B to VLAN 33. Assign both an IPv4 address and IPv6 address to VLAN-interface 33.

```
[DeviceC] vlan 33
[DeviceC-vlan33] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 33
[DeviceC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[DeviceC-GigabitEthernet1/0/2] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface33] ip address 33.1.1.2 24
[DeviceC-Vlan-interface33] ipv6 address 33::2 64
[DeviceC-Vlan-interface33] quit
```

Set the router ID to 5.5.5.5.

```
[DeviceC] router id 5.5.5.5
```

Enable OSPF on VLAN-interface 32 and VLAN-interface 33.

```
[DeviceC] ospf 1
[DeviceC-ospf-1] import-route direct
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ospf 1 area 0
[DeviceC-Vlan-interface32] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface33] ospf 1 area 0
[DeviceC-Vlan-interface33] quit
```

Enable OSPFv3 on VLAN-interface 32 and VLAN-interface 33.

```
[DeviceC] ospfv3 1
[DeviceC-ospfv3-1] import-route direct
[DeviceC-ospfv3-1] area 0
[DeviceC-ospfv3-1-area-0.0.0.0] quit
[DeviceC-ospfv3-1] quit
[DeviceC] interface vlan-interface 32
[DeviceC-Vlan-interface32] ospfv3 1 area 0
[DeviceC-Vlan-interface32] quit
[DeviceC] interface vlan-interface 33
[DeviceC-Vlan-interface32] ospfv3 1 area 0
[DeviceC-Vlan-interface33] quit
```

Create VLAN 22. Assign GigabitEthernet 1/0/3 that connects to Network1 to VLAN 22. Assign both an IPv4 address and IPv6 address to VLAN-interface 22.

```
[DeviceC] vlan 22
[DeviceC-vlan22] quit
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 22
[DeviceC-GigabitEthernet1/0/3] undo port trunk permit vlan 1
```

```
[DeviceC-GigabitEthernet1/0/3] quit
[DeviceC] interface vlan-interface 22
[DeviceC-Vlan-interface22] ip address 22.1.1.1 24
[DeviceC-Vlan-interface22] ipv6 address 22::1 64
[DeviceC-Vlan-interface22] quit
```

Configuring Device D

Create Layer 2 aggregate interface Bridge-Aggregation 3 and configure the interface to operate in dynamic mode.

```
<DeviceD> system-view
[DeviceD] interface bridge-aggregation 3
[DeviceD-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation3] quit
```

Assign interfaces HundredGigE 1/0/1 through HundredGigE 1/0/4 to aggregation group 3.

```
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[DeviceD-if-range] port link-aggregation group 3
[DeviceD-if-range] quit
```

Create VLAN 100.

```
[DeviceD] vlan 100
[DeviceD-vlan100] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 100.

```
[DeviceD] interface bridge-aggregation 3
[DeviceD-Bridge-Aggregation3] port link-type trunk
[DeviceD-Bridge-Aggregation3] port trunk permit vlan 100
[DeviceD-Bridge-Aggregation3] undo port trunk permit vlan 1
[DeviceD-Bridge-Aggregation3] quit
```

Verifying the configuration

Verifying the status of the M-LAG system

Verify that the peer-link interface and M-LAG interfaces are working correctly on Device A and Device B. Use Device A as an example.

Display summary information about the IPP and M-LAG interface.

```
[DeviceA] display m-lag summary
Flags: A -- Aggregate interface down, B -- No peer M-LAG interface configured
       C -- Configuration consistency check failed

Peer-link interface: BAGG1
Peer-link interface state (cause): UP
Keepalive link state (cause): UP

                    M-LAG interface information
M-LAG IF    M-LAG group  Local state (cause)  Peer state  Remaining down time(s)
BAGG3       1            UP                   UP          -
```

Verify that keepalive link is working correctly.

```
[DeviceA] display m-lag keepalive
```

```
Neighbor keepalive link status: Up
Neighbor is alive for: 64765 s 28 ms
Keepalive packet transmission status:
  Sent: Successful
  Received: Successful
Last received keepalive packet information:
  Source IP address: 21.1.1.2
  Time: 2021/01/17 17:10:52
  Action: Accept

M-LAG keepalive parameters:
Destination IP address: 21.1.1.2
Source IP address: 21.1.1.1
Keepalive UDP port : 6400
Keepalive VPN name : N/A
Keepalive interval : 1000 ms
Keepalive timeout  : 5 sec
Keepalive hold time: 3 sec
```

Display the M-LAG system settings.

```
<Sysname> display m-lag system
                     System information
Local system number: 1                      Peer system number: 2
Local system MAC: 0002-0002-0002            Peer system MAC: 0002-0002-0002
Local system priority: 123                  Peer system priority: 123
Local bridge MAC: 3cd4-3ce1-0200            Peer bridge MAC: 3cd4-437d-0300
Local effective role: Primary               Peer effective role: Secondary
Health level: 0
Standalone mode on split: Disabled
In standalone mode: No

                     System timer information
Timer                      State       Value (s)    Remaining time (s)
Auto recovery              Disabled    -            -
Restore delay              Disabled    30           -
Consistency-check delay    Disabled    15           -
Standalone delay           Disabled    -            -
Role to None delay         Disabled    60           -
```

Display detailed information about the IPP and M-LAG interfaces.

```
[DeviceA] display m-lag verbose
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- PeerLink_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired

Peer-link interface/Peer-link interface ID: BAGG1/1
State: UP
Cause: -
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/3 (27), GE1/0/4 (32)
```

```
Peer Selected ports indexes: 125, 130

M-LAG interface/M-LAG group ID: BAGG3/1
Local M-LAG interface state: UP
Peer M-LAG interface state: UP
M-LAG group state: UP
Local M-LAG interface down cause: -
Remaining M-LAG DOWN time: -
Local M-LAG interface LACP MAC: Config=N/A, Effective=0002-0002-0002
Peer M-LAG interface LACP MAC: Config=N/A, Effective=0002-0002-0002
Local M-LAG interface LACP priority: Config=32768, Effective=123
Peer M-LAG interface LACP priority: Config=32768, Effective=123
Local DRCP flags/Peer DRCP flags: ABDFG/ABDFG
Local Selected ports (index): GE1/0/1 (12), GE1/0/2 (13)
Peer Selected ports indexes: 56, 57
```

Verifying the routing protocols

Display the OSPF neighbors of Device A.

```
[DeviceA] display ospf peer

         OSPF Process 1 with Router ID 3.3.3.3
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 4.4.4.4         101.1.1.2       1   36         Full/DR           Vlan101
 5.5.5.5         32.1.1.2        1   38         Full/DR           Vlan32
```

Display the OSPFv3 neighbors of Device A.

```
[DeviceA] display ospfv3 peer

               OSPFv3 Process 1 with Router ID 3.3.3.3

 Area: 0.0.0.0
----------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 4.4.4.4         1   Full/DR           00:00:36  0      Vlan101
 5.5.5.5         1   Full/DR           00:00:35  0      Vlan32
```

Display the OSPF neighbors of Device B.

```
[DeviceB] display ospf peer

         OSPF Process 1 with Router ID 4.4.4.4
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         101.1.1.1       1   32         Full/BDR          Vlan101
 5.5.5.5         33.1.1.2        1   33         Full/DR           Vlan33
```

Display the OSPFv3 neighbors of Device B.

```
[DeviceB] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 4.4.4.4

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 3.3.3.3         1   Full/BDR          00:00:35  0      Vlan101
 5.5.5.5         1   Full/DR           00:00:38  0      Vlan33
```

Display the OSPF neighbors of Device C.

```
[DeviceC] display ospf peer

         OSPF Process 1 with Router ID 5.5.5.5
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         32.1.1.1        1   32         Full/DR           Vlan32
 4.4.4.4         33.1.1.1        1   38         Full/DR           Vlan33
```

Display the OSPFv3 neighbors of Device C.

```
[DeviceC] display ospfv3 peer

              OSPFv3 Process 1 with Router ID 5.5.5.5

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 3.3.3.3         1   Full/DR           00:00:37  0      Vlan32
 4.4.4.4         1   Full/DR           00:00:34  0      Vlan33
```

Verifying that Server 1 and Server 2 can communicate with Network 1

Server 1 and Server 2 can communicate with Network 1 through both IPv4 and IPv6 addresses.

Verifying that Server 1 and Server 2 can still communicate with Network 1 when the uplink interface of Device A or Device B fails

Disconnect the interface connecting Device A to Device C. Server 1 and Server 2 can still communicate with Network 1 (transient packet loss occurs during the traffic switchover process).

Configuration files

- Device A:

```
#
 router id 3.3.3.3
#
ospf 1
```

```
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
ospfv3 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
vlan 1
#
vlan 32
#
vlan 100 to 101
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
 port m-lag group 1
#
interface Vlan-interface32
 ip address 32.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 32::1/64
#
interface Vlan-interface100
 ip address 100.1.1.100 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 mac-address 0000-0010-0010
 ipv6 address FE80::80 link-local
 ipv6 address 100::100/64
#
interface Vlan-interface101
 ip address 101.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 101::1/64
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port link-aggregation group 1
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 21.1.1.1 255.255.255.0
 ipv6 address 21::1/64
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 32
#
 m-lag system-mac 0002-0002-0002
 m-lag system-number 1
 m-lag system-priority 123
 m-lag keepalive ip destination 21.1.1.2 source 21.1.1.1
 m-lag mad exclude interface GigabitEthernet1/0/5
 m-lag mad exclude interface Vlan-interface100
```

```
 m-lag mad exclude interface Vlan-interface101
#
```

- Device B:

```
#
 router id 4.4.4.4
#
ospf 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
ospfv3 1
 import-route direct
 silent-interface Vlan-interface100
 area 0.0.0.0
#
vlan 1
#
vlan 33
#
vlan 100 to 101
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
 port m-lag group 1
#
interface Vlan-interface33
 ip address 33.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 33::1/64
#
interface Vlan-interface100
 ip address 100.1.1.100 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 mac-address 0000-0010-0010
 ipv6 address FE80::80 link-local
 ipv6 address 100::100/64
```

```
#
interface Vlan-interface101
 ip address 101.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 101::2/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 combo enable fiber
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/5
 port link-mode route
 ip address 21.1.1.2 255.255.255.0
 ipv6 address 21::2/64
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 33
#
 m-lag system-mac 0002-0002-0002
 m-lag system-number 2
```

```
 m-lag system-priority 123
 m-lag keepalive ip destination 21.1.1.1 source 21.1.1.2
 m-lag mad exclude interface GigabitEthernet1/0/5
 m-lag mad exclude interface Vlan-interface100
 m-lag mad exclude interface Vlan-interface101
#
```

- Device C:

```
#
 router id 5.5.5.5
#
ospf 1
 import-route direct
 area 0.0.0.0
#
ospfv3 1
 import-route direct
 area 0.0.0.0
#
vlan 1
#
vlan 22
#
vlan 32 to 33
#
interface Vlan-interface22
 ip address 22.1.1.1 255.255.255.0
 ipv6 address 22::1/64
#
interface Vlan-interface32
 ip address 32.1.1.1 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 32::2/64
#
interface Vlan-interface33
 ip address 33.1.1.2 255.255.255.0
 ospf 1 area 0.0.0.0
 ospfv3 1 area 0.0.0.0
 ipv6 address 33::2/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 32
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 33
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 22
#
```

- Device D:

```
#
vlan 1
#
vlan 100
#
interface Bridge-Aggregation3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port link-aggregation group 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
```

```
 port link-aggregation group 3
#
```

Contents

Introduction

Mirror On Drop (MOD) can detect packet drops during the forwarding process on the device. When a packet is dropped, MOD can send the packet drop reason and the characteristics of the dropped packet to the collector.

This document provides examples for configuring MOD.

Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of MOD.

General restrictions and guidelines

When you configure MOD follow these restrictions and guidelines:

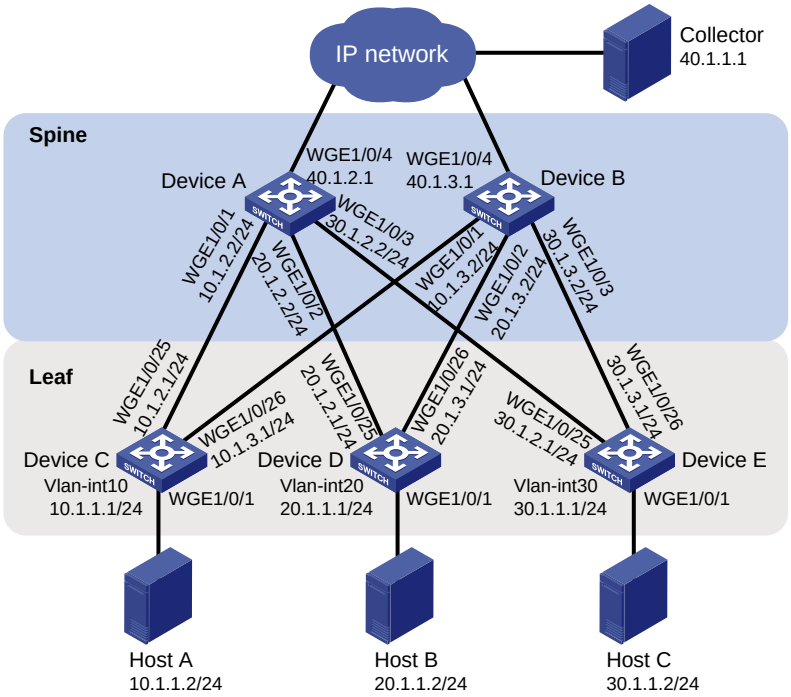
- Only one ACL can be specified for a flow group.
- Because a flow can belong to only one flow group, make sure the same flow is not assigned to more than one flow group when specifying ACLs.
- MOD takes effect only on packets matching ACLs referenced by flow groups.
- To delete an applied flow group, first remove the application and then delete the flow group.
- You cannot modify the name or mode of an existing flow group.

Example: Configuring simple MOD

Network configuration

As shown in Figure 1, the network uses a spine-leaf architecture. Configure simple MOD on the spine device and leaf devices to identify whether packets are dropped during the forwarding process on the devices.

Figure 1 Network diagram



Analysis

To generate flow entries based on the flow group, configure the flow group mode to simple MOD.

Configure simple MOD to monitor packet drops based on the reason list.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported

MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch	Not supported

E152C switch E500C switch series E500D switch series	
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC IE4300-12P-PWR IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring Device A

Configuring IP addresses for interfaces

Configure interfaces Twenty-FiveGigE 1/0/1 through Twenty-FiveGigE 1/0/3 to operate in Layer 3 mode, and configure an IP address for each interface.

```
<DeviceA> system-view
[DeviceA] interface twenty-fivegige 1/0/1
[DeviceA-Twenty-FiveGigE1/0/1] port link-mode route
[DeviceA-Twenty-FiveGigE1/0/1] ip address 10.1.2.2 24
[DeviceA-Twenty-FiveGigE1/0/1] quit
[DeviceA] interface twenty-fivegige 1/0/2
[DeviceA-Twenty-FiveGigE1/0/2] port link-mode route
[DeviceA-Twenty-FiveGigE1/0/2] ip address 20.1.2.2 24
[DeviceA-Twenty-FiveGigE1/0/2] quit
[DeviceA] interface twenty-fivegige 1/0/3
[DeviceA-Twenty-FiveGigE1/0/3] port link-mode route
[DeviceA-Twenty-FiveGigE1/0/3] ip address 30.1.2.2 24
[DeviceA-Twenty-FiveGigE1/0/3] quit
```

Configuring a routing protocol

Configure OSPF.

```
[DeviceA] ospf 1 router-id 1.1.1.1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
```

```
[DeviceA-ospf-1-area-0.0.0.0] network 20.1.2.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 30.1.2.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

Configuring a flow group

Create advanced IPv4 ACL 3000, and configure a rule to match packets with destination IP address 10.0.0.10 for the ACL.

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule permit ip destination 30.1.1.2 0
[DeviceA-acl-ipv4-adv-3000] quit
```

Create flow group 2 in simple MOD mode and configure it to reference ACL 3000.

```
[DeviceA] telemetry flow-group 2 mode simple-mod
[DeviceA-telemetry-flow-group-2] if-match acl 3000
```

Configure the flow group to generate flow entries based on the destination IP address.

```
[DeviceA-telemetry-flow-group-2] template destination-ip
[DeviceA-telemetry-flow-group-2] quit
```

Set the flow entry aging time to 10 minutes.

```
[DeviceA] telemetry flow-group aging-time 10
```

Apply flow group 2.

```
[DeviceA] telemetry apply flow-group 2
```

Configuring simple MOD

Configure the device ID for simple MOD as 10.1.2.2.

```
[DeviceA] telemetry mod
[DeviceA-telemetry-mod] device-id 10.1.2.2
```

Specify UDP for simple MOD to use to send packets to the collector.

```
[DeviceA-telemetry-mod] transport-protocol udp
```

Encapsulate the packets sent to the collector by simple MOD with the following information: source IP address 10.1.2.2, destination IP address 40.1.1.1, source port number 1000, and destination port number 2333.

```
[DeviceA-telemetry-mod] collector source-ip 10.1.2.2 destination-ip 40.1.1.1 source-port
1000 destination-port 2333
```

Configure simple MOD to monitor all packet drop reasons.

```
[DeviceA-telemetry-mod] reason-list all
[DeviceA-telemetry-mod] quit
[DeviceA] quit
```

Configuring Device B, Device C, Device D, and Device E

Configure Device B, Device C, Device D, and Device E in the same way Device A is configured except for the following items:

- Interface IP addresses.
- OSPF router ID and network segments.

Device ID for simple MOD.

Source IP address encapsulated in the packets sent to the collector.

Verifying the configuration

Verifying the configuration on Device A

Display the ACL configuration.

```
<DeviceA> display acl 3000
Advanced IPv4 ACL 3000, 1 rule,
ACL's step is 5, start ID is 0
 rule 0 permit ip destination 30.1.1.2 0
```

Display the flow group configuration.

```
<DeviceA> display telemetry flow-group 2
Flow group 2 (Successful)
  ACL       : 3000
  Template  : destination-ip
  Mode      : Simple MOD
Aging time: 10 minutes
Rate limit:  -
Max-entry :  -
```

Display the simple MOD configuration.

```
<DeviceA> display telemetry mod
Status          : Successful
Drop reason list:
  ipv4-dip-miss
  ip-multicast-error
  unknown-vlan
  tunnel-header-error
  parity-error
  higig-header-error
  invalid-tpid
  ipv6-dip-miss
Device ID          : 10.1.2.2
Transport protocol : UDP
Collector
  Source IP        : 10.1.2.2
  Destination IP   : 40.1.1.1
  Source port      : 1000
  Destination port : 2333
```

Verifying the configuration on Device B, Device C, Device D, and Device E

The configurations on Device B, Device C, Device D, and Device E are the same as the configuration on Device A except for interface IP addresses, OSPF configuration, the device ID for simple MOD, and the source IP address encapsulated in the packets sent to the collector. (Details not shown.)

Analyzing MOD packets received by the collector

Ping Host C from Device A.

```
<DeviceA> ping 30.1.1.2
Ping 30.1.1.2 (30.1.1.2): 56 data bytes, press CTRL+C to break
56 bytes from 30.1.1.2: icmp_seq=0 ttl=255 time=4.703 ms
56 bytes from 30.1.1.2: icmp_seq=1 ttl=255 time=1.636 ms
56 bytes from 30.1.1.2: icmp_seq=2 ttl=255 time=1.733 ms
56 bytes from 30.1.1.2: icmp_seq=3 ttl=255 time=1.662 ms
56 bytes from 30.1.1.2: icmp_seq=4 ttl=255 time=1.606 ms

--- Ping statistics for 30.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.606/2.268/4.703/1.218 ms
```

Modify the configuration of Device E.

```
<DeviceE> system-view
[DeviceE] ospf 1
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] undo network 30.1.2.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

Ping Host C from Device A.

```
<DeviceA> ping 30.1.1.2
Ping 30.1.1.2 (30.1.1.2): 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 30.1.1.2 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

When a packet destined for Host C is dropped during the forwarding process on the spine device and leaf devices, the collector can receive the packet drop reason and the characteristics of the dropped packet from the devices.

In this example, the packet drop information received by the collector showed that Device A dropped packets and the packet drop reason is ipv4-dip-miss. This indicates that there is no route on Device A to Host C. After you recover the OSPF configuration on Device E, Host C can receive the packets.

Configuration files

- Device A:

```
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 20.1.2.0 0.0.0.255
```

```
  network 30.1.2.0 0.0.0.255
#
interface Twenty-FiveGigE1/0/1
 port link-mode route
 ip address 10.1.2.2 255.255.255.0
#
interface Twenty-FiveGigE1/0/2
 port link-mode route
 ip address 20.1.2.2 255.255.255.0
#
interface Twenty-FiveGigE1/0/3
 port link-mode route
 ip address 30.1.2.2 255.255.255.0
#
acl advanced 3000
 rule 0 permit ip destination 30.1.1.2 0
#
telemetry mod
 reason-list all
 device-id 10.1.2.2
 collector source-ip 10.1.2.2 destination-ip 40.1.1.1 source-port 1000
destination-port 2333
#
telemetry flow-group 21 mode simple-mod
 if-match acl 3000
 template destination-ip
#
 telemetry apply flow-group 2
 telemetry flow-group aging-time 10
#
```

- Device B, Device C, Device D, and Device E:

  The configurations on Device B, Device C, Device D, and Device E are the same as the configuration on Device A except for interface IP addresses, OSPF router ID and network segments, the device ID for simple MOD, and the source IP address encapsulated in the packets sent to the collector. (Details not shown.)

Contents

Overview

MPLS L2VPN provides point-to-point and point-to-multipoint connections. This chapter describes only the MPLS L2VPN technologies that provide point-to-point connections. This document describes configuration examples for implementing MPLS L2VPN in the following ways:

- CCC
- Static
- LDP
- BGP

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of MPLS L2VPN.

Restrictions and guidelines

Before you configure MPLS, you must change the device's operating mode by using the **switch-mode** command and restart the device for the following switches:

- S6812 series
- S6813 series
- S5560X-EI series
- S5560X-HI series
- S5500V2-EI series
- MS4520V2-30F
- MS4520V2-30C
- MS4520V2-54C
- S6520X-HI series
- S6520X-EI series
- S6520X-SI series
- S6520-SI series
- S5000-EI series
- MS4600 series

In a non-IRF environment, use the **`switch-mode 3`** command to switch the device to MPLS mode.

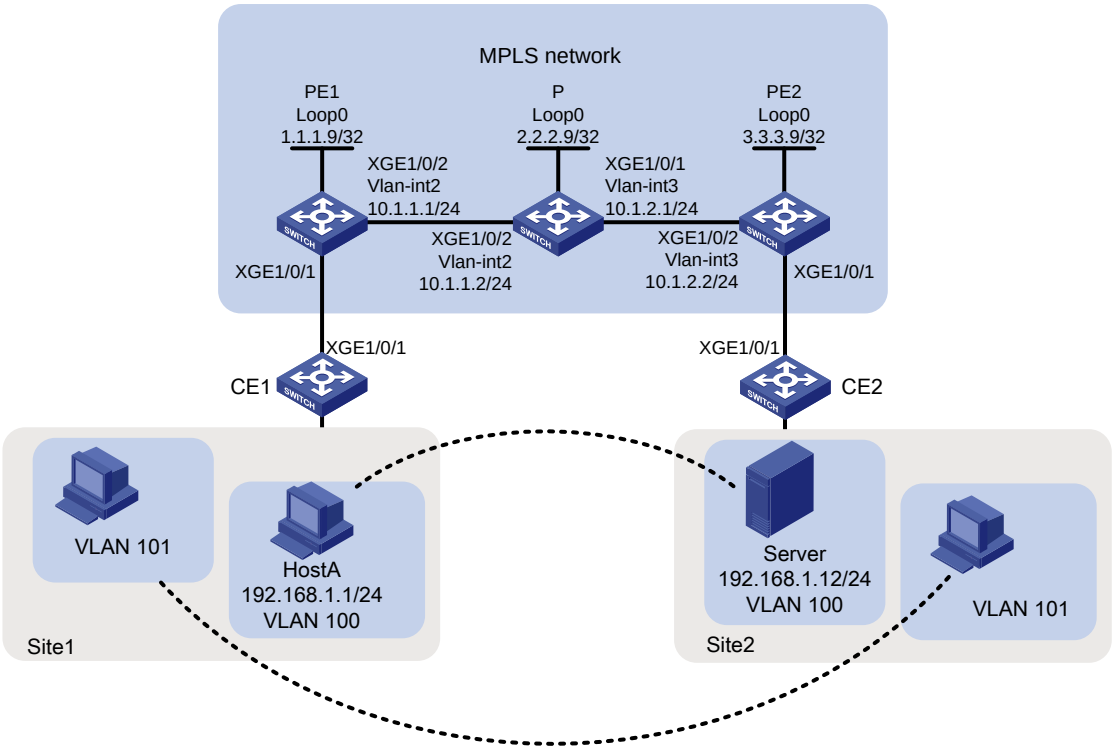
In an IRF environment, use the **`switch-mode 4`** command to switch the device to MPLS-IRF mode.

Example: Configuring CCC-based MPLS L2VPN

Network configuration

As shown in Figure 1, customer network sites Site1 and Site2, located at different physical locations, access the carrier MPLS network via devices CE1 and CE2, respectively. Users want host communication between the two sites to be unaware of the MPLS network's existence, as if both parties are in the same local area network (LAN). To achieve this, configure MPLS L2VPN using the CCC method to allow communication between VLAN 100 at Site1 and VLAN 100 at Site2, as well as between VLAN 101 at Site1 and VLAN 101 at Site2, while preventing communication between different VLANs.

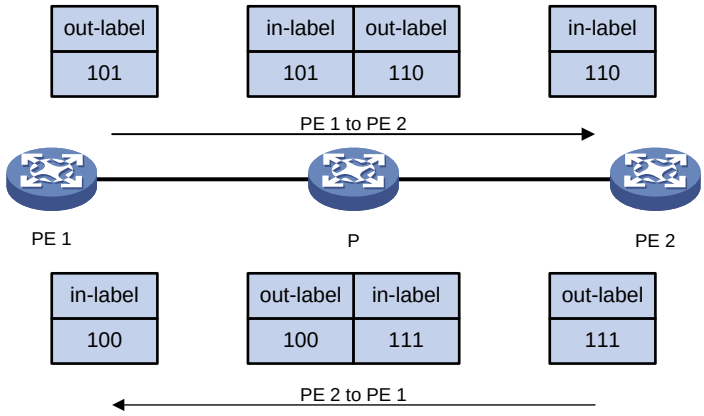
Figure 1 Network diagram



Analysis

To establish an MPLS L2VPN connection by using the CCC mode, configure an ingress label and an egress label for each CCC connection on the PEs, and a bidirectional static LSP on the P device. The egress label must match the next hop's ingress label. Take the traffic of VLAN 100 as an example. As shown in Figure 2, in the direction from PE 1 to PE 2, PE 1's egress label and P's ingress label are 101, and P's egress label and PE 2's ingress label are 110. In the direction from PE 2 to PE 1, PE 2's egress label and P's ingress label are 111, and P's egress label and PE 1's ingress label are 100.

Figure 2 Label switching for VLAN100 traffic



Applicable hardware and software versions

Table 1 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI	Unsupported

Hardware	Software version
S5500V3-48P-SI	
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported

Hardware	Software version
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring interface attributes and enabling basic MPLS capabilities

- Configure PE 1:

  # Configure an LSR ID.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable MPLS L2VPN globally.

  ```
  [PE1] l2vpn enable
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port Ten-GigabitEthernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Create VLAN-interface 2 and enable MPLS on the interface.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  <P> system-view
  [P] interface loopback 0
  [P-LoopBack0] ip address 2.2.2.9 32
  [P-LoopBack0] quit
  [P] mpls lsr-id 2.2.2.9
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

  ```
  [P] vlan3
  [P-vlan3] port Ten-GigabitEthernet1/0/1
  [P-vlan3] quit
  ```

  # Configure VLAN-interface 3 and enable MPLS on the interface.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] ip address 10.1.2.1 24
  [P-Vlan-interface3] mpls enable
  [P-Vlan-interface3] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[P] vlan2
[P-vlan2] port Ten-GigabitEthernet1/0/2
[P-vlan2] quit
```

Configure VLAN-interface 2 and enable MPLS on the interface.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] mpls enable
[P-Vlan-interface2] quit
```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  <PE2> system-view
  [PE2] interface loopback 0
  [PE2-LoopBack0] ip address 3.3.3.9 32
  [PE2-LoopBack0] quit
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable MPLS L2VPN globally.

  ```
  [PE2] l2vpn enable
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/2 to VLAN 3.

  ```
  [PE2] vlan 3
  [PE2-vlan3] port Ten-GigabitEthernet 1/0/2
  [PE2-vlan3] quit
  ```

  # Configure VLAN-interface 3 and enable MPLS on the interface.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] ip address 10.1.2.2 24
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] quit
  ```

Creating a CCC remote connection on a PE and configuring a static LSP on the P device

- Configure PE 1:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

  ```
  [PE1] interface ten-gigabitethernet1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 101 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 101.

  ```
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 101
  [PE1-Ten-GigabitEthernet1/0/1-srv101] encapsulation s-vid 101
  [PE1-Ten-GigabitEthernet1/0/1-srv101] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna** and create a CCC remote connection named **ccc** with an incoming label of 100, an outgoing label of 101, and a next-hop address of 10.1.1.2 in the VPN. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this CCC remote connection.

  ```
  [PE1] xconnect-group vpna
  [PE1-xcg-vpna] connection ccc
  [PE1-xcg-vpna-ccc] ccc in-label 100 out-label 101 nexthop 10.1.1.2
  [PE1-xcg-vpna-ccc] ac interface ten-gigabitethernet 1/0/1 service-instance 100
  ```

```
[PE1-xcg-vpna-ccc] quit
[PE1-xcg-vpna] quit
```

Create a cross-connect group named **vpnb** and create a remote CCC connection named **ccc** with an incoming label of 200, an outgoing label of 201, and a next-hop address of 10.1.1.2 in the VPN. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this remote CCC connection.

```
[PE1] xconnect-group vpnb
[PE1-xcg-vpnb] connection ccc
[PE1-xcg-vpnb-ccc] ccc in-label 200 out-label 201 nexthop 10.1.1.2
[PE1-xcg-vpnb-ccc] ac interface ten-gigabitethernet 1/0/1 service-instance 101
[PE1-xcg-vpnb-ccc] quit
[PE1-xcg-vpnb] quit
```

- Configure the P device:

  # Configure a static LSP to forward packets from PE 1 to PE 2 that carry traffic from VLAN 100.

  ```
  [P] static-lsp transit pe1-pe2-100 in-label 101 nexthop 10.1.2.2 out-label 110
  ```

  # Configure a static LSP to forward packets from PE 1 to PE 2 that carry traffic from VLAN 101.

  ```
  [P] static-lsp transit pe1-pe2-101 in-label 201 nexthop 10.1.2.2 out-label 210
  ```

  # Configure a static LSP to forward packets from PE 2 to PE 1 that carry traffic from VLAN 100.

  ```
  [P] static-lsp transit pe2-pe1-100 in-label 111 nexthop 10.1.1.1 out-label 100
  ```

  # Configure a static LSP to forward packets from PE 2 to PE 1 that carry traffic from VLAN 101.

  ```
  [P] static-lsp transit pe2-pe1-101 in-label 211 nexthop 10.1.1.1 out-label 200
  ```

- Configure PE 2:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

  ```
  [PE2] interface ten-gigabitethernet1/0/1
  [PE2-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 101 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 101.

  ```
  [PE2-Ten-GigabitEthernet1/0/1] service-instance 101
  [PE2-Ten-GigabitEthernet1/0/1-srv101] encapsulation s-vid 101
  [PE2-Ten-GigabitEthernet1/0/1-srv101] quit
  [PE2-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna** and create a remote CCC connection named **ccc** with an incoming label of 110, an outgoing label of 111, and a next-hop address of to 10.1.2.1 in the VPN. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this remote CCC connection.

  ```
  [PE2] xconnect-group vpna
  [PE2-xcg-vpna] connection ccc
  [PE2-xcg-vpna-ccc] ccc in-label 110 out-label 111 nexthop 10.1.2.1
  [PE2-xcg-vpna-ccc] ac interface ten-gigabitethernet 1/0/1 service-instance 100
  [PE2-xcg-vpna-ccc] quit
  [PE2-xcg-vpna] quit
  ```

  # Create a cross-connect group named **vpnb** and create a remote CCC connection named **ccc** with an incoming label of 210, an outgoing label of 211, and a next-hop address of 10.1.2.1 in the VPN. Bind service instance 101 on Ten-GigabitEthernet 1/0/1 to this remote CCC connection.

  ```
  [PE2] xconnect-group vpnb
  ```

```
[PE2-xcg-vpnb] connection ccc
[PE2-xcg-vpnb-ccc] ccc in-label 210 out-label 211 nexthop 10.1.2.1
[PE2-xcg-vpnb-ccc] ac interface ten-gigabitethernet 1/0/1 service-instance 101
[PE2-xcg-vpnb-ccc] quit
[PE2-xcg-vpnb] quit
```

Connecting CEs to PEs

- Configure CE 1:

  # Configure Ten-GigabitEthernet 1/0/1 as a trunk port and permit VLAN 100and VLAN 101.

```
<CE1> system-view
[CE1] vlan 100 to 101
[CE1] interface Ten-GigabitEthernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 101
```

- Configure CE 2:

  # Configure Ten-GigabitEthernet 1/0/1 as a trunk port and permit VLAN 100and VLAN 101.

```
<CE2> system-view
[CE2] vlan 100 to 101
[CE2] interface Ten-GigabitEthernet 1/0/1
[CE2-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE2-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 101
```

Verifying the configuration

Display PW information on PE 1. The output shows that two PW connections have been established. The value for the PW ID/Rmt Site field is -, and the value for the Proto field is Static, indicating that the PW connections are remote CCC connections.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.1.2        -                 100/101         Static  M     1        Up

Xconnect-group Name: vpnb
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.1.2        -                 200/201         Static  M     1        Up
```

Verify that PW information can also be displayed on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.2.1        -                 110/111         Static  M     1        Up

Xconnect-group Name: vpnb
```

```
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
10.1.2.1        -                 210/211         Static  M     1        Up
```

Use ping to identify whether host A and the server and hosts in VLAN 101 at the two sites can reach each other. If the ping operation succeeds, the L2VPN is established successfully.

Configuration files

- CE 1

```
#
vlan 100 to 101
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 to 101
#
```

- PE 1

```
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
 l2vpn enable
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
 service-instance 101
  encapsulation s-vid 101
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
xconnect-group vpna
 connection ccc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
  ccc in-label 100 out-label 101 nexthop 10.1.1.2
#
xconnect-group vpnb
```

```
 connection ccc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 101
  ccc in-label 200 out-label 201 nexthop 10.1.1.2
#
```

- P

```
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 3
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
 static-lsp transit pe1-pe2-100 in-label 101 nexthop 10.1.2.2 out-label 110
 static-lsp transit pe1-pe2-101 in-label 201 nexthop 10.1.2.2 out-label 210
 static-lsp transit pe2-pe1-100 in-label 111 nexthop 10.1.1.1 out-label 100
 static-lsp transit pe2-pe1-101 in-label 211 nexthop 10.1.1.1 out-label 200
#
```

- PE 2

```
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
 l2vpn enable
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
```

```
 ip address 10.1.2.2 255.255.255.0
 mpls enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
 service-instance 101
  encapsulation s-vid 101
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
xconnect-group vpna
 connection ccc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
  ccc in-label 110 out-label 111 nexthop 10.1.2.1
#
xconnect-group vpnb
 connection ccc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 101
  ccc in-label 210 out-label 211 nexthop 10.1.2.1
#
```

- CE 2

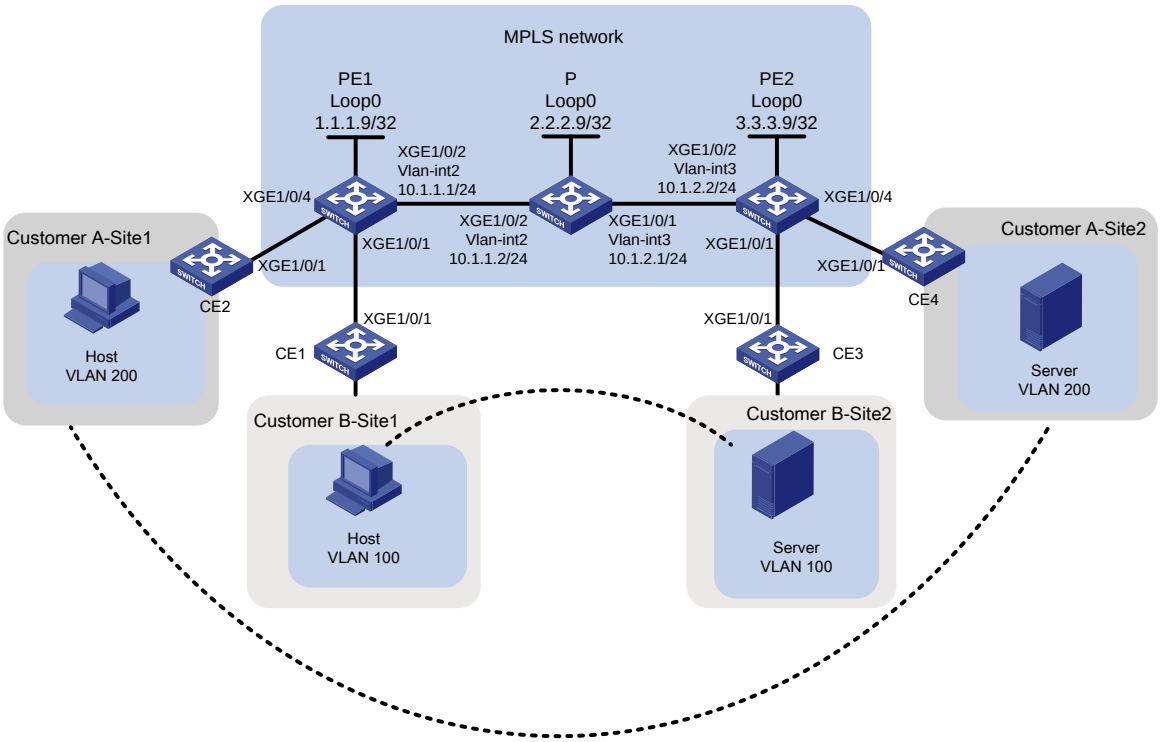
```
#
vlan 100 to 101
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 to 101
#
```

Example: Configuring static MPLS L2VPN

Network configuration

As shown in Figure 3, the MPLS network provides L2VPN services between different sites for User A and User B, with each user having only two fixed sites. Configure static MPLS L2VPN to enable communication between VLAN 200 of Site 1 and Site 2 for User A, and between VLAN 100 of Site 1 and Site 2 for User B.

Figure 3 Network diagram



Analysis

- Static MPLS L2VPN uses a two-layer label structure. In this example, the inner layer label is generated through manual configuration, and the outer layer label is dynamically generated by LDP.
- To ensure normal label exchange, make sure the incoming label configured at the local PE matches the outgoing label configured at the remote PE when you configure static connections for the same user. For User A, the outgoing label at Site 1 and the incoming label at Site 2 are 200, and the incoming label at Site 1 and the outgoing label at Site 2 are 201. For User B, the outgoing label at Site 1 and the incoming label at Site 2 are 100, and the incoming label at Site 1 and the outgoing label at Site 2 are 101.

Applicable hardware and software versions

Table 2 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx

Hardware	Software version
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported

Hardware	Software version
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices on the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port Ten-GigabitEthernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Configure VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] quit
  ```

Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

- Configure the P device:

  # Configure a loopback interface address.

  ```
  <P> system-view
  [P] interface loopback 0
  [P-LoopBack0] ip address 2.2.2.9 32
  [P-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

  ```
  [P] vlan 2
  [P-vlan2] port Ten-GigabitEthernet1/0/2
  [P-vlan2] quit
  ```

  # Configure VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] ip address 10.1.1.2 24
  [P-Vlan-interface2] quit
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

  ```
  [P] vlan 3
  [P-vlan3] port Ten-GigabitEthernet1/0/1
  [P-vlan3] quit
  ```

  # Configure VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] ip address 10.1.2.1 24
  [P-Vlan-interface3] quit
  ```

  # Configure OSPF on the P device for establishing LSPs.

  ```
  [P] ospf
  [P-ospf-1] area 0
  [P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
  [P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
  [P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
  [P-ospf-1-area-0.0.0.0] quit
  [P-ospf-1] quit
  ```

- Configure PE 2:

  # Configure a loopback interface address.

  ```
  <PE2> system-view
  [PE2] interface loopback 0
  [PE2-LoopBack0] ip address 3.3.3.9 32
  [PE2-LoopBack0] quit
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/2 to VLAN 3.

  ```
  [PE2] vlan 3
  [PE2-vlan3] port Ten-GigabitEthernet 1/0/2
  [PE2-vlan3] quit
  ```

Configure VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] quit
```

Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configuring basic MPLS capabilities and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

  ```
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable LDP globally.

  ```
  [PE1] mpls ldp
  [PE1-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] mpls ldp enable
  [PE1-Vlan-interface2] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

  ```
  [P] mpls ldp
  [P-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] mpls enable
  [P-Vlan-interface2] mpls ldp enable
  [P-Vlan-interface2] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] mpls enable
  [P-Vlan-interface3] mpls ldp enable
  [P-Vlan-interface3] quit
  ```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable LDP globally.

  ```
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

Enable MPLS and LDP on VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] mpls enable
[PE2-Vlan-interface3] mpls ldp enable
[PE2-Vlan-interface3] quit
```

Enabling MPLS L2VPN and configuring inner labels for different users

- Configure PE 1:

  # Enable MPLS L2VPN globally.

  ```
  [PE1] l2vpn enable
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

  ```
  [PE1] interface ten-gigabitethernet1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna** and create a cross-connect named **svc**. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this cross-connect and create a static PW inside the cross-connect to associate the AC and PW.

  ```
  [PE1] xconnect-group vpna
  [PE1-xcg-vpna] connection svc
  [PE1-xcg-vpna-svc] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
  [PE1-xcg-vpna-svc] peer 3.3.3.9 pw-id 100 in-label 101 out-label 100
  [PE1-xcg-vpna-svc-3.3.3.9-100] quit
  [PE1-xcg-vpna-svc] quit
  [PE1-xcg-vpna] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/4 to match packets with VLAN tag 200.

  ```
  [PE1] interface ten-gigabitethernet1/0/4
  [PE1-Ten-GigabitEthernet1/0/4] service-instance 200
  [PE1-Ten-GigabitEthernet1/0/4-srv200] encapsulation s-vid 200
  [PE1-Ten-GigabitEthernet1/0/4-srv200] quit
  [PE1-Ten-GigabitEthernet1/0/4] quit
  ```

  # Create a cross-connect group named **vpnb** and create a cross-connect named **svc**. Bind service instance 100 on Ten-GigabitEthernet 1/0/4 to this cross-connect and create a static PW inside the cross-connect to associate the AC and PW.

  ```
  [PE1] xconnect-group vpnb
  [PE1-xcg-vpnb] connection svc
  [PE1-xcg-vpnb-svc] ac interface Ten-GigabitEthernet 1/0/4 service-instance 200
  [PE1-xcg-vpnb-svc] peer 3.3.3.9 pw-id 200 in-label 201 out-label 200
  [PE1-xcg-vpnb-svc-3.3.3.9-200] quit
  [PE1-xcg-vpnb-svc] quit
  [PE1-xcg-vpnb] quit
  ```

- Configure PE 2:

  # Enable MPLS L2VPN globally.

  ```
  [PE2] l2vpn enable
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

```
[PE2] interface ten-gigabitethernet1/0/1
[PE2-Ten-GigabitEthernet1/0/1] service-instance 100
[PE2-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/1-srv100] quit
[PE2-Ten-GigabitEthernet1/0/1] quit
```

Create service instance 200 on Ten-GigabitEthernet 1/0/4 to match packets with VLAN tag 200.

```
[PE2] interface ten-gigabitethernet1/0/4
[PE2-Ten-GigabitEthernet1/0/4] service-instance 200
[PE2-Ten-GigabitEthernet1/0/4-srv200] encapsulation s-vid 200
[PE2-Ten-GigabitEthernet1/0/4-srv200] quit
[PE2-Ten-GigabitEthernet1/0/4] quit
```

Create a cross-connect group named **vpna** and create a cross-connect named **svc**. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this cross-connect and create a static PW inside the cross-connect to associate the AC and PW.

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] connection svc
[PE2-xcg-vpna-svc] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
[PE2-xcg-vpna-svc] peer 1.1.1.9 pw-id 100 in-label 100 out-label 101
[PE2-xcg-vpna-svc-1.1.1.9-100] quit
[PE2-xcg-vpna-svc] quit
[PE2-xcg-vpna] quit
```

Create a cross-connect group named **vpnb** and create a cross-connect named **svc**. Bind service instance 100 on Ten-GigabitEthernet 1/0/4 to this cross-connect and create a static PW inside the cross-connect to associate the AC and PW.

```
[PE2] xconnect-group vpnb
[PE2-xcg-vpnb] connection svc
[PE2-xcg-vpnb-svc] ac interface Ten-GigabitEthernet 1/0/4 service-instance 200
[PE2-xcg-vpnb-svc] peer 1.1.1.9 pw-id 200 in-label 200 out-label 201
[PE2-xcg-vpnb-svc-1.1.1.9-200] quit
[PE2-xcg-vpnb-svc] quit
[PE2-xcg-vpnb] quit
```

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the site to pass through. The following uses CE1 as an example. Configure other CEs in the same way CE1 is configured.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface Ten-GigabitEthernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Verifying the configuration

Display PW information on PE1 to verify that two static PWs have been set up.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect
```

```
Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
3.3.3.9         100        101/100         Static M     1          Up

Xconnect-group Name: vpnb
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
3.3.3.9         200        201/200         Static M     1          Up
```

Verify that static PW information can also be the displayed on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
1.1.1.9         100        100/101         Static M     1          Up

Xconnect-group Name: vpnb
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
1.1.1.9         200        200/201         Static M     1          Up
```

Identify whether the host and server of the same user can communicate between different sites. If they can, the L2VPN has been successfully established.

Configuration files

- CE 1

```
#
vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100
#
```

- CE 2

```
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 200
#
```

- CE 3

```
#
vlan 100
#
```

```
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100
#
```

- CE 4

```
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 200
#
```

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
vlan 100
#
vlan 200
#
mpls ldp
#
 l2vpn enable
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 service-instance 200
  encapsulation s-vid 200
#
xconnect-group vpna
 connection svc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
  peer 3.3.3.9 pw-id 100 in-label 101 out-label 100
#
xconnect-group vpnb
 connection svc
  ac interface Ten-GigabitEthernet1/0/4 service-instance 200
  peer 3.3.3.9 pw-id 200 in-label 201 out-label 200
#
```

- P

```
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 3
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
```

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
vlan 100
#
vlan 200
#
mpls ldp
#
 l2vpn enable
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 service-instance 200
  encapsulation s-vid 200
#
xconnect-group vpna
 connection svc
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
```

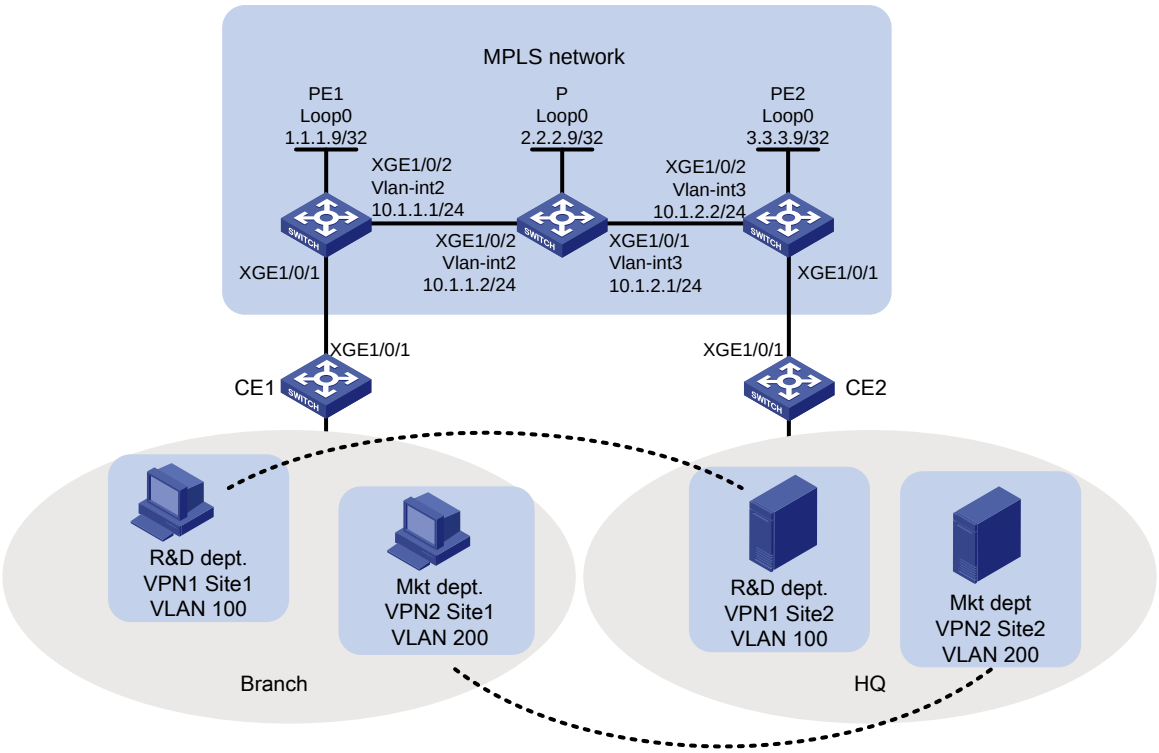
```
  peer 1.1.1.9 pw-id 100 in-label 100 out-label 101
#
xconnect-group vpnb
 connection svc
  ac interface Ten-GigabitEthernet1/0/4 service-instance 200
  peer 1.1.1.9 pw-id 200 in-label 200 out-label 201
#
```

Example: Configuring LDP-based MPLS L2VPN

Network configuration

As shown Figure 4, the carrier provides L2VPN service for a user over the MPLS network. The user has R&D and marketing departments in branch offices and headquarters. They require setup of separate VPN connections between these departments by using LDP-based MPLS L2VPN to achieve data isolation.

Figure 4 Network diagram



Analysis

- LDP-based MPLS L2VPN uses a two-layer label structure, where both the inner and outer labels are dynamically generated by LDP.

- Configure a service instance and corresponding match rules on the downstream port of the PE devices to identify packets from the customer network that require transmission through an MPLS L2VPN tunnel.

Applicable hardware and software versions

Table 3 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series	Unsupported

Hardware	Software version
S5120V2-LI Series	
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices in the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port Ten-GigabitEthernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Create VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] quit
  ```

  # Configure OSPF on PE 1 for establishing LSPs.

  ```
  [PE1] ospf
  [PE1-ospf-1] area 0
  [PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
  [PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
  [PE1-ospf-1-area-0.0.0.0] quit
  [PE1-ospf-1] quit
  ```

- Configure the P device:

  # Configure a loopback interface address.

  ```
  <P> system-view
  [P] interface loopback 0
  [P-LoopBack0] ip address 2.2.2.9 32
  [P-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

  ```
  [P] vlan 2
  [P-vlan2] port Ten-GigabitEthernet1/0/2
  [P-vlan2] quit
  ```

  # Configure VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] ip address 10.1.1.2 24
  [P-Vlan-interface2] quit
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

  ```
  [P] vlan 3
  [P-vlan3] port Ten-GigabitEthernet1/0/1
  [P-vlan3] quit
  ```

  # Configure VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] ip address 10.1.2.1 24
  ```

```
[P-Vlan-interface3] quit
```

Configure OSPF on the P device for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

- Configure PE 2:

  # Configure a loopback interface address.

  ```
  <PE2> system-view
  [PE2] interface loopback 0
  [PE2-LoopBack0] ip address 3.3.3.9 32
  [PE2-LoopBack0] quit
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/2 to VLAN 3.

  ```
  [PE2] vlan 3
  [PE2-vlan3] port Ten-GigabitEthernet 1/0/2
  [PE2-vlan3] quit
  ```

  # Create VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] ip address 10.1.2.2 24
  [PE2-Vlan-interface3] quit
  ```

  # Configure OSPF on PE 2 for establishing LSPs.

  ```
  [PE2] ospf
  [PE2-ospf-1] area 0
  [PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
  [PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
  [PE2-ospf-1-area-0.0.0.0] quit
  [PE2-ospf-1] quit
  ```

Configuring basic MPLS capabilities and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

  ```
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable LDP globally.

  ```
  [PE1] mpls ldp
  [PE1-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] mpls ldp enable
  [PE1-Vlan-interface2] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

```
[P] mpls ldp
[P-ldp] quit
```

Enable MPLS and LDP VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls enable
[P-Vlan-interface2] mpls ldp enable
[P-Vlan-interface2] quit
```

Enable MPLS and LDP on VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls enable
[P-Vlan-interface3] mpls ldp enable
[P-Vlan-interface3] quit
```

- Configure PE 2.

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable LDP globally.

  ```
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] mpls ldp enable
  [PE2-Vlan-interface3] quit
  ```

Configuring service instances for data from different departments and bind them to different MPLS L2VPNs

- Configure PE 1:

  # Enable MPLS L2VPN globally.

  ```
  [PE1] l2vpn enable
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 100.

  ```
  [PE1] interface ten-gigabitethernet1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200.

  ```
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna** and create a cross-connect named **ldp**. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this cross-connect and create an LDP PW in the cross-connect to associate the AC and PW.

  ```
  [PE1] xconnect-group vpna
  [PE1-xcg-vpna] connection ldp
  [PE1-xcg-vpna-ldp] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
  [PE1-xcg-vpna-ldp] peer 3.3.3.9 pw-id 100
  [PE1-xcg-vpna-ldp-3.3.3.9-100] quit
  [PE1-xcg-vpna-ldp] quit
  ```

```
[PE1-xcg-vpna] quit
```

Create a cross-connect group named **vpnb** and create a cross-connect named **ldp**. Bind service instance 200 on Ten-GigabitEthernet 1/0 1 to this cross-connect and create an LDP PW in the cross-connect to associate the AC and PW.

```
[PE1] xconnect-group vpnb
[PE1-xcg-vpnb] connection ldp
[PE1-xcg-vpnb-ldp] ac interface Ten-GigabitEthernet 1/0/1 service-instance 200
[PE1-xcg-vpnb-ldp] peer 3.3.3.9 pw-id 200
[PE1-xcg-vpnb-ldp-3.3.3.9-200] quit
[PE1-xcg-vpnb-ldp] quit
[PE1-xcg-vpnb] quit
```

- Configure PE 2:

  # Enable MPLS L2VPN globally.

  ```
  [PE2] l2vpn enable
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 100.

  ```
  [PE2] interface ten-gigabitethernet1/0/1
  [PE2-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200.

  ```
  [PE2-Ten-GigabitEthernet1/0/1] service-instance 200
  [PE2-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
  [PE2-Ten-GigabitEthernet1/0/1-srv200] quit
  [PE2-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna** and create a cross-connect named **ldp**. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to this cross-connect and create an LDP PW in the cross-connect to associate the AC and PW.

  ```
  [PE2] xconnect-group vpna
  [PE2-xcg-vpna] connection ldp
  [PE2-xcg-vpna-ldp] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
  [PE2-xcg-vpna-ldp] peer 1.1.1.9 pw-id 100
  [PE2-xcg-vpna-ldp-1.1.1.9-100] quit
  [PE2-xcg-vpna-ldp] quit
  [PE2-xcg-vpna] quit
  ```

  # Create a cross-connect group named **vpnb** and create a cross-connect named **ldp**. Bind service instance 100 on Ten-GigabitEthernet 1/0 1 to this cross-connect and create an LDP PW in the cross-connect to associate the AC and PW.

  ```
  [PE2] xconnect-group vpnb
  [PE2-xcg-vpnb] connection ldp
  [PE2-xcg-vpnb-ldp] ac interface Ten-GigabitEthernet 1/0/1 service-instance 200
  [PE2-xcg-vpnb-ldp] peer 1.1.1.9 pw-id 200
  [PE2-xcg-vpnb-ldp-1.1.1.9-200] quit
  [PE2-xcg-vpnb-ldp] quit
  [PE2-xcg-vpnb] quit
  ```

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the site to pass through. The following uses CE1 as an example. Configure CE2 in the same way CE1 is configured.

```
<CE1> system-view
```

```
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] vlan 200
[CE1-vlan200] quit
[CE1] interface Ten-GigabitEthernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Verifying the configuration

Display L2VPN connection information on PE 1 to verify that two LDP PWs have been set up.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
3.3.3.9         100        65663/65663     LDP    M     1          Up

Xconnect-group Name: vpnb
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
3.3.3.9         200        65662/65662     LDP    M     1          Up
```

Verify that LDP PW information can also be displayed on PE 2.

```
[PE2] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
1.1.1.9         100        65663/65663     LDP    M     1          Up

Xconnect-group Name: vpnb
Peer            PW ID      In/Out Label    Proto  Flag  Link ID    State
1.1.1.9         200        65662/65662     LDP    M     1          Up
```

Identify whether the host and server of the same user can communicate between different sites. If they can, the L2VPN has been successfully established.

Configuration files

- CE 1 and CE 2

```
#
 vlan 100
#
 vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 100 200
#
```

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls ldp
#
 l2vpn enable
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
 service-instance 200
  encapsulation s-vid 200
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
xconnect-group vpna
 connection ldp
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
  peer 3.3.3.9 pw-id 100
#
xconnect-group vpnb
 connection ldp
  ac interface Ten-GigabitEthernet1/0/1 service-instance 200
  peer 3.3.3.9 pw-id 200
#
```

- P

```
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 3
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls ldp
```

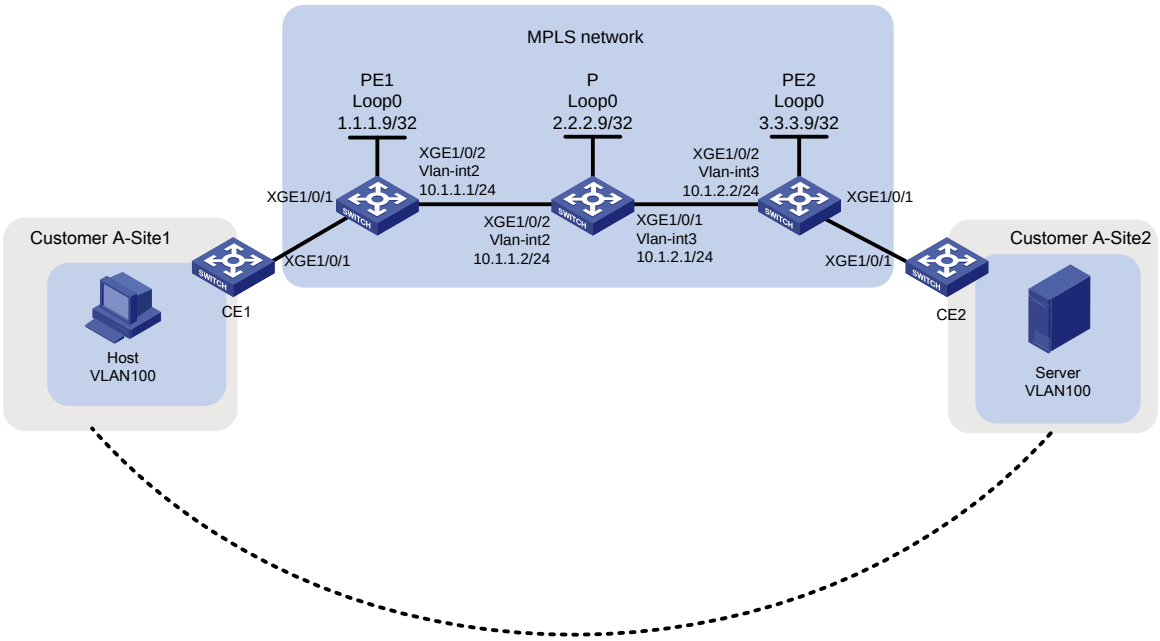
```
#
 l2vpn enable
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
 service-instance 200
  encapsulation s-vid 200
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
xconnect-group vpna
 connection ldp
  ac interface Ten-GigabitEthernet1/0/1 service-instance 100
  peer 1.1.1.9 pw-id 100
#
xconnect-group vpnb
 connection ldp
  ac interface Ten-GigabitEthernet1/0/1 service-instance 200
  peer 1.1.1.9 pw-id 200
#
```

Example: Configuring BGP-based MPLS L2VPN

Network configuration

As shown in Figure 5, the MPLS network provides MPLS L2VPN services to the user. The user has two sites deployed and the number might be expanded to 10. To connect the two sites over VPN and reserve VPN resources for the remaining 8 sites, configure BGP-based MPLS L2VPN.

Figure 5 Network diagram



Analysis

- BGP-based MPLS L2VPN uses a two-layer label structure, where the inner label is generated by BGP and the outer label is dynamically created using LDP.
- To enable PEs to use BGP for exchanging private network labels, create service instances and IBGP connections on each PE and configure them as BGP peers.
- To reduce the configuration workload when you increase the number of sites to 10, set the label block size to 10.

Applicable hardware and software versions

Table 4 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C	Release 6628Pxx series

Hardware	Software version
MS4520V2-54C	
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported

Hardware	Software version
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices on the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port Ten-GigabitEthernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Create VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] quit
  ```

  # Configure OSPF on PE 1 for establishing LSPs.

  ```
  [PE1] ospf
  [PE1-ospf-1] area 0
  [PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
  [PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
  ```

```
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

- Configure the P device:

  # Configure a loopback interface address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[P] vlan2
[P-vlan2] port Ten-GigabitEthernet1/0/2
[P-vlan2] quit
```

  # Configure VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

```
[P] vlan3
[P-vlan3] port Ten-GigabitEthernet1/0/1
[P-vlan3] quit
```

  # Configure VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] quit
```

  # Configure OSPF on the P device for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

- Configure PE 2:

  # Configure a loopback interface address.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/2 to VLAN 3.

```
[PE2] vlan 3
[PE2-vlan3] port Ten-GigabitEthernet 1/0/2
[PE2-vlan3] quit
```

  # Create VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] quit
```

  # Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configuring basic MPLS capabilities and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

  ```
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable MPLS L2VPN and LDP globally.

  ```
  [PE1] l2vpn enable
  [PE1] mpls ldp
  [PE1-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] mpls ldp enable
  [PE1-Vlan-interface2] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

  ```
  [P] mpls ldp
  [P-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] mpls enable
  [P-Vlan-interface2] mpls ldp enable
  [P-Vlan-interface2] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] mpls enable
  [P-Vlan-interface3] mpls ldp enable
  [P-Vlan-interface3] quit
  ```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable MPLS L2VPN and LDP globally.

  ```
  [PE2] l2vpn enable
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] mpls ldp enable
  ```

```
[PE2-Vlan-interface3] quit
```

Establishing an IBGP connection between PEs and configuring BGP PWs

- Configure PE 1:

  # Create an IBGP connection to PE 2.

  ```
  [PE1] bgp 100
  [PE1-bgp] peer 3.3.3.9 as-number 100
  [PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
  ```

  # Enable BGP to advertise L2VPN information to PE 2.

  ```
  [PE1-bgp] address-family l2vpn
  [PE1-bgp-l2vpn] peer 3.3.3.9 enable
  [PE1-bgp-l2vpn] quit
  [PE1-bgp] quit
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

  ```
  [PE1] interface ten-gigabitethernet1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

  # Create a cross-connect group named **vpna**, create local site site 1, and create a BGP PW from site 1 to remote site site 2. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to the PW.

  ```
  [PE1] xconnect-group vpna
  [PE1-xcg-vpna] auto-discovery bgp
  [PE1-xcg-vpna-auto] route-distinguisher 2:2
  [PE1-xcg-vpna-auto] vpn-target 2:2 export-extcommunity
  [PE1-xcg-vpna-auto] vpn-target 2:2 import-extcommunity
  [PE1-xcg-vpna-auto] site 1 range 10 default-offset 0
  [PE1-xcg-vpna-auto-1] connection remote-site-id 2
  [PE1-xcg-vpna-auto-1-2] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
  [PE1-xcg-vpna-auto-1-2] return
  ```

- Configure PE 2:

  # Create an IBGP connection to PE 1, and enable BGP to advertise L2VPN information to PE 1.

  ```
  [PE2] bgp 100
  [PE2-bgp] peer 1.1.1.9 as-number 100
  [PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
  [PE2-bgp] address-family l2vpn
  [PE2-bgp-l2vpn] peer 1.1.1.9 enable
  [PE2-bgp-l2vpn] quit
  [PE2-bgp] quit
  ```

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets with VLAN tag 100.

  ```
  [PE2] interface ten-gigabitethernet1/0/1
  [PE2-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE2-Ten-GigabitEthernet1/0/1-srv100] quit
  [PE2-Ten-GigabitEthernet1/0/1] quit
  ```

Create a cross-connect group named **vpna**, create local site site 2, and create a BGP PW from site 2 to remote site site 1. Bind service instance 100 on Ten-GigabitEthernet 1/0/1 to the PW.

```
[PE2] xconnect-group vpna
[PE2-xcg-vpna] auto-discovery bgp
[PE2-xcg-vpna-auto] route-distinguisher 2:2
[PE2-xcg-vpna-auto] vpn-target 2:2 export-extcommunity
[PE2-xcg-vpna-auto] vpn-target 2:2 import-extcommunity
[PE2-xcg-vpna-auto] site 2 range 10 default-offset 0
[PE2-xcg-vpna-auto-2] connection remote-site-id 1
[PE2-xcg-vpna-auto-2-1] ac interface Ten-GigabitEthernet 1/0/1 service-instance 100
[PE2-xcg-vpna-auto-2-1] return
```

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the local site to pass through. The following uses CE1 as an example. Configure other CEs in the same way CE1 is configured.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface Ten-GigabitEthernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100
```

Verifying the configuration

Display PW information on PE1 to verify that a BGP PW has been set up.

```
<PE1> display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
3.3.3.9         2                 65538/65537     BGP     M     1        Up
```

Verify that PW information can also be displayed on PE 2.

```
<PE2> display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 1, 1 up, 0 blocked, 0 down, 0 defect

Xconnect-group Name: vpna
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
1.1.1.9         1                 65537/65538     BGP     M     1        Up
```

Use ping to identify whether hosts within the two sites can reach each other. If the ping operation succeeds, the VPN is created successfully.

Configuration files

- CE 1 and CE 2

  ```
  #
  ```

```
 vlan 100
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls ldp
#
 l2vpn enable
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 3.3.3.9 enable
#
xconnect-group vpna
 auto-discovery bgp
  route-distinguisher 2:2
```

```
  vpn-target 2:2 export-extcommunity
  vpn-target 2:2 import-extcommunity
  site 1 range 10 default-offset 0
   connection remote-site-id 2
    ac interface Ten-GigabitEthernet1/0/1 service-instance 100
#
```

- P

```
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
 mpls lsr-id 2.2.2.9
#
vlan 2
#
vlan 3
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
```

```
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls ldp
#
 l2vpn enable
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 1.1.1.9 enable
#
xconnect-group vpna
 auto-discovery bgp
  route-distinguisher 2:2
  vpn-target 2:2 export-extcommunity
  vpn-target 2:2 import-extcommunity
  site 2 range 10 default-offset 0
   connection remote-site-id 1
    ac interface Ten-GigabitEthernet1/0/1 service-instance 100
#
```

Contents

Overview

Virtual Private LAN Service (VPLS) delivers a point-to-multipoint L2VPN service over an MPLS or IP backbone. The provider backbone emulates a switch to connect all geographically dispersed sites of each customer network. The backbone is transparent to the customer sites. The sites can communicate with each other as if they were on the same LAN.

VPLS has the following networking models:

- **Full mesh**—Suitable for MPLS backbone networks with a simple architecture and fewer PEs. The following networking modes are available under this model:
  - **LDP**—Uses the LDP protocol as the signaling protocol, suitable for scenarios with a small number of sites and the number of sites is fixed.
  - **BGP auto-discovery with LDP signaling**—Uses the BGP protocol to automatically discover remote PEs, and then uses the LDP protocol as the signaling protocol, suitable for scenarios with many sites but the number of sites is fixed.
  - **BGP**—Uses extended BGP as the signaling protocol, suitable for scenarios with a large number of sites and the need for expansion.
- **H-VPLS**—Suitable for MPLS backbone networks with a complex architecture and a large number of PEs. This model uses a hierarchical network structure that contains UPEs and NPEs. A UPE is responsible for customer site access and establishing connections with the nearest NPE, and NPEs are fully interconnected logically. UPEs exchange packets with remote sites through NPEs. The following networking modes are available under this model:
  - **LSP access**—Packets are transmitted over an LSP tunnel, suitable for scenarios where UPEs support VPLS.
  - **QinQ access**—Packets are encapsulated with an outer VLAN tag before being transmitted over an LSP tunnel, suitable for scenarios where UPE devices do not support VPLS.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of VPLS.

Restrictions and guidelines

Before you configure MPLS, you must change the device's operating mode by using the **switch-mode** command and restart the device for the following switches:

- S6812 series
- S6813 series
- S5560X-EI series
- S5560X-HI series
- S5500V2-EI series
- MS4520V2-30F
- MS4520V2-30C
- MS4520V2-54C
- S6520X-HI series

- S6520X-EI series
- S6520X-SI series
- S6520-SI series
- S5000-EI series
- MS4600 series

In a non-IRF environment, use the **switch-mode 3** command to switch the device to MPLS mode.

In an IRF environment, use the **switch-mode 4** command to switch the device to MPLS-IRF mode.

PEs do not transparently transmit LACP or LLDP protocol packets over a VPLS network.

If STP is globally enabled on a PE, the PE transparently transmits STP packets over the VPLS network only after you use the **stp transparent enable** command to enable BPDU transparent transmission on a port. For more information about the **stp transparent enable** command, see STP commands in *Layer 2—LAN Switching Command Reference*.

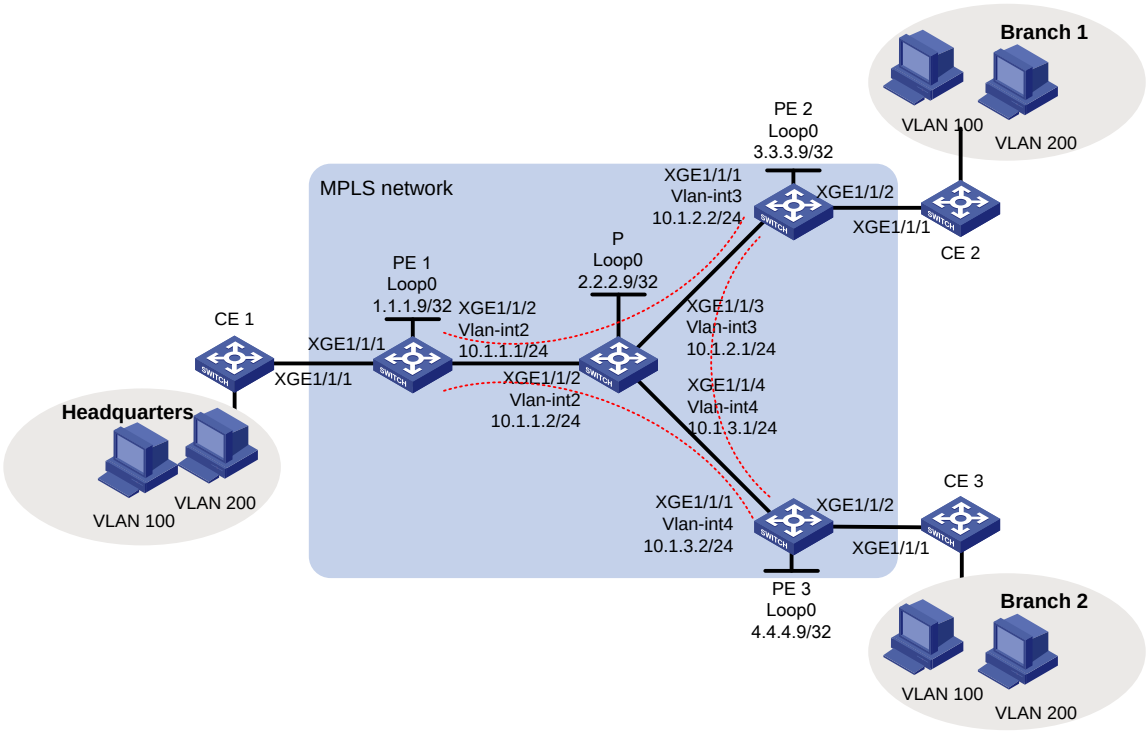
Example: Configuring full-mesh VPLS (LDP signaling)

Network configuration

As shown in Figure 1, a company has three offices in different locations: headquarters and two branches. The company requires the provider to offer a Layer 2 VPN service that interconnects the three offices at Layer 2, allowing them to share internal resources.

The company has few branches and will not expand further. To meet user requirements, configure LDP-based VPLS to enable communication between the three sites at Layer 2.

Figure 1 Network diagram



Analysis

- Deploy MPLS on the backbone network and use LSP as the public tunnel.
- Establish LDP PWs between the PEs for full-mesh VPLS.
- Configure a service instance and corresponding match rules on the downlink port of each PE device to identify packets from the customer network that require a VPLS tunnel for transmission.
- To achieve VLAN isolation between sites, create VSIs **user_a** and **user_b** and bind them to VLAN 100 and VLAN 200, respectively.

Applicable hardware and software versions

Table 1 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported

Hardware	Software version
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported

Hardware	Software version
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices on the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port ten-gigabitethernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Create VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] quit
  ```

  # Configure OSPF on PE 1 for establishing LSPs.

  ```
  [PE1] ospf
  [PE1-ospf-1] area 0
  [PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
  [PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
  [PE1-ospf-1-area-0.0.0.0] quit
  [PE1-ospf-1] quit
  ```

- Configure PE 2:

  # Configure a loopback interface address.

  ```
  <PE2> system-view
  [PE2] interface loopback 0
  [PE2-LoopBack0] ip address 3.3.3.9 32
  [PE2-LoopBack0] quit
  ```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

  ```
  [PE2] vlan 3
  [PE2-vlan3] port ten-gigabitethernet 1/0/1
  [PE2-vlan3] quit
  ```

  # Create VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] ip address 10.1.2.2 24
  [PE2-Vlan-interface3] quit
  ```

  # Configure OSPF on PE 2 for establishing LSPs.

  ```
  [PE2] ospf
  [PE2-ospf-1] area 0
  [PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
  ```

```
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

- Configure PE 3:

  # Configure a loopback interface address.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 4.4.4.9 32
[PE3-LoopBack0] quit
```

  # Create VLAN 4 and add Ten-GigabitEthernet 1/0/1 to VLAN 4.

```
[PE3] vlan 4
[PE3-vlan4] port ten-gigabitethernet 1/0/1
[PE3-vlan4] quit
```

  # Create VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.1.3.2 24
[PE3-Vlan-interface4] quit
```

  # Configure OSPF on PE 3 for establishing LSPs.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

- Configure the P device:

  # Configure a loopback interface address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[P] vlan 2
[P-vlan2] port ten-gigabitethernet 1/0/2
[P-vlan2] quit
```

  # Configure VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
```

  # Create VLAN 3 and add Ten-GigabitEthernet 3/0/1 to VLAN 3.

```
[P] vlan 3
[P-vlan3] port ten-gigabitethernet 1/0/3
[P-vlan3] quit
```

  # Configure VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] quit
```

  # Create VLAN 4 and add Ten-GigabitEthernet 1/0/4 to VLAN 4.

```
[P] vlan 4
[P-vlan4] port ten-gigabitethernet 1/0/4
[P-vlan4] quit
```

Configure VLAN-interface 4.

```
[P] interface vlan-interface 4
[P-Vlan-interface4] ip address 10.1.3.1 24
[P-Vlan-interface4] quit
```

Configure OSPF on the P device for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring basic MPLS and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

  ```
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable LDP globally.

  ```
  [PE1] mpls ldp
  [PE1-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] mpls ldp enable
  [PE1-Vlan-interface2] quit
  ```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable LDP globally.

  ```
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] mpls ldp enable
  [PE2-Vlan-interface3] quit
  ```

- Configure PE 3:

  # Configure an LSR ID.

  ```
  [PE3] mpls lsr-id 4.4.4.9
  ```

  # Enable LDP globally.

  ```
  [PE3] mpls ldp
  [PE3-ldp] quit
  ```

Enable MPLS and LDP on VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] mpls enable
[PE3-Vlan-interface4] mpls ldp enable
[PE3-Vlan-interface4] quit
```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

  ```
  [P] mpls ldp
  [P-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] mpls enable
  [P-Vlan-interface2] mpls ldp enable
  [P-Vlan-interface2] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] mpls enable
  [P-Vlan-interface3] mpls ldp enable
  [P-Vlan-interface3] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 4.

  ```
  [P] interface vlan-interface 4
  [P-Vlan-interface4] mpls enable
  [P-Vlan-interface4] mpls ldp enable
  [P-Vlan-interface4] quit
  ```

Creating a VSI and configuring LDP PWs

- Configure PE 1:

  # Enable MPLS L2VPN globally.

  ```
  [PE1] l2vpn enable
  ```

  # Configure VSI **user_a** that uses LDP as the PW signaling protocol.

  ```
  [PE1] vsi user_a
  [PE1-vsi-user_a] pwsignaling ldp
  ```

  # Establish PWs to PE 2 and PE 3.

  ```
  [PE1-vsi-user_a-ldp] peer 3.3.3.9 pw-id 500
  [PE1-vsi-user_a-ldp-3.3.3.9-500] quit
  [PE1-vsi-user_a-ldp] peer 4.4.4.9 pw-id 500
  [PE1-vsi-user_a-ldp-4.4.4.9-500] quit
  [PE1-vsi-user_a-ldp] quit
  [PE1-vsi-user_a] quit
  ```

  # Configure VSI **user_b** that uses LDP as the PW signaling protocol.

  ```
  [PE1] vsi user_b
  [PE1-vsi-user_b] pwsignaling ldp
  ```

  # Establish PWs to PE 2 and PE 3.

  ```
  [PE1-vsi-user_b-ldp] peer 3.3.3.9 pw-id 600
  [PE1-vsi-user_b-ldp-3.3.3.9-600] quit
  [PE1-vsi-user_b-ldp] peer 4.4.4.9 pw-id 600
  ```

```
[PE1-vsi-user_b-ldp-4.4.4.9-600] quit
[PE1-vsi-user_b-ldp] quit
[PE1-vsi-user_b] quit
```

- Configure PE 2:

  # Enable MPLS L2VPN globally.

```
[PE2] l2vpn enable
```

  # Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[PE2] vsi user_a
[PE2-vsi-user_a] pwsignaling ldp
```

  # Establish PWs to PE 1 and PE 3.

```
[PE2-vsi-user_a-ldp] peer 1.1.1.9 pw-id 500
[PE2-vsi-user_a-ldp-1.1.1.9-500] quit
[PE2-vsi-user_a-ldp] peer 4.4.4.9 pw-id 500
[PE2-vsi-user_a-ldp-4.4.4.9-500] quit
[PE2-vsi-user_a-ldp] quit
[PE2-vsi-user_a] quit
```

  # Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[PE2] vsi user_b
[PE2-vsi-user_b] pwsignaling ldp
```

  # Establish PWs to PE 1 and PE 3.

```
[PE2-vsi-user_b-ldp] peer 1.1.1.9 pw-id 600
[PE2-vsi-user_b-ldp-1.1.1.9-600] quit
[PE2-vsi-user_b-ldp] peer 4.4.4.9 pw-id 600
[PE2-vsi-user_b-ldp-4.4.4.9-600] quit
[PE2-vsi-user_b-ldp] quit
[PE2-vsi-user_b] quit
```

- Configure PE 3:

  # Enable MPLS L2VPN globally.

```
[PE3] l2vpn enable
```

  # Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[PE3] vsi user_a
[PE3-vsi-user_a] pwsignaling ldp
```

  # Establish PWs to PE 1 and PE 2.

```
[PE3-vsi-user_a-ldp] peer 1.1.1.9 pw-id 500
[PE3-vsi-user_a-ldp-1.1.1.9-500] quit
[PE3-vsi-user_a-ldp] peer 3.3.3.9 pw-id 500
[PE3-vsi-user_a-ldp-3.3.3.9-500] quit
[PE3-vsi-user_a-ldp] quit
[PE3-vsi-user_a] quit
```

  # Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[PE3] vsi user_b
[PE3-vsi-user_b] pwsignaling ldp
```

  # Establish PWs to PE 1 and PE 2.

```
[PE3-vsi-user_b-ldp] peer 1.1.1.9 pw-id 600
[PE3-vsi-user_b-ldp-1.1.1.9-600] quit
[PE3-vsi-user_b-ldp] peer 3.3.3.9 pw-id 600
[PE3-vsi-user_b-ldp-3.3.3.9-600] quit
```

```
[PE3-vsi-user_b-ldp] quit
[PE3-vsi-user_b] quit
```

Configuring service instances for data from different VLANs and bind them to different VSIs

- Configure PE 1:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE1] interface ten-gigabitethernet 1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] xconnect vsi user_a
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] xconnect vsi user_b
  [PE1-Ten-GigabitEthernet1/0/1-srv200] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

- Configure PE 2:

  # Create service instance 100 on Ten-GigabitEthernet 2/0/2 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE2] interface ten-gigabitethernet 1/0/2
  [PE2-Ten-GigabitEthernet1/0/2] service-instance 100
  [PE2-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
  [PE2-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
  [PE2-Ten-GigabitEthernet1/0/2-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE2-Ten-GigabitEthernet1/0/2] service-instance 200
  [PE2-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
  [PE2-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
  [PE2-Ten-GigabitEthernet1/0/2-srv200] quit
  [PE2-Ten-GigabitEthernet1/0/2] quit
  ```

- Configure PE 3:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE3] interface ten-gigabitethernet 1/0/2
  [PE3-Ten-GigabitEthernet1/0/2] service-instance 100
  [PE3-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
  [PE3-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
  [PE3-Ten-GigabitEthernet1/0/2-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE3-Ten-GigabitEthernet1/0/2] service-instance 200
  [PE3-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
  [PE3-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
  [PE3-Ten-GigabitEthernet1/0/2-srv200] quit
  [PE3-Ten-GigabitEthernet1/0/2] quit
  ```

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the site to pass through. The following uses CE 1 as an example. Configure CE2 and CE2 in the same way CE1 is configured.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] vlan 200
[CE1-vlan200] quit
[CE1] interface ten-gigabitethernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Verifying the configuration

Verifying the public network LSPs

Execute the **display mpls ldp lsp** command to verify that the LSPs have been established.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal
Statistics:
  FECs: 4      Ingress LSPs: 3     Transit LSPs: 3     Egress LSPs: 1

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
                   -/1151(L)
                   -/1151(L)
2.2.2.9/32         -/3             10.1.1.2        Vlan2
                   1151/3          10.1.1.2        Vlan2
                   -/1150(L)
                   -/1150(L)
3.3.3.9/32         -/1150          10.1.1.2        Vlan2
                   1150/1150       10.1.1.2        Vlan2
                   -/3(L)
                   -/1149(L)
4.4.4.9/32         -/1149          10.1.1.2        Vlan2
                   1149/1149       10.1.1.2        Vlan2
                   -/1149(L)
                   -/3(L)
```

Verifying PW status

Execute the **display l2vpn pw** command on each PE. The output shows that a PW has been established and in up state.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 4
4 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

VSI Name: user_a
```

```
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
3.3.3.9         500               131198/131198   LDP     M     64       Up
4.4.4.9         500               131199/1150     LDP     M     65       Up

VSI Name: user_b
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
3.3.3.9         600               131196/131196   LDP     M     64       Up
4.4.4.9         600               131197/1147     LDP     M     65       Up
```

Use ping to identify whether hosts within the same VLAN but at different sites can reach each other. If the ping operation succeeds, the VPLS is created successfully.

Configuration files

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 3.3.3.9 pw-id 500
  peer 4.4.4.9 pw-id 500
#
vsi user_b
 pwsignaling ldp
  peer 3.3.3.9 pw-id 600
  peer 4.4.4.9 pw-id 600
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
```

```
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.9 pw-id 500
  peer 4.4.4.9 pw-id 500
#
vsi user_b
 pwsignaling ldp
  peer 1.1.1.9 pw-id 600
  peer 4.4.4.9 pw-id 600
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
```

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
```

- PE 3

```
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
#
 mpls lsr-id 4.4.4.9
#
vlan 4
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.9 pw-id 500
  peer 3.3.3.9 pw-id 500
#
vsi user_b
 pwsignaling ldp
  peer 1.1.1.9 pw-id 600
  peer 3.3.3.9 pw-id 600
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface4
 ip address 10.1.3.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
```

```
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
```

- P

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 4
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface4
 ip address 10.1.3.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
```

```
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 4
#
```

- CE 1 through CE 3

```
#
vlan 100
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 200
#
```

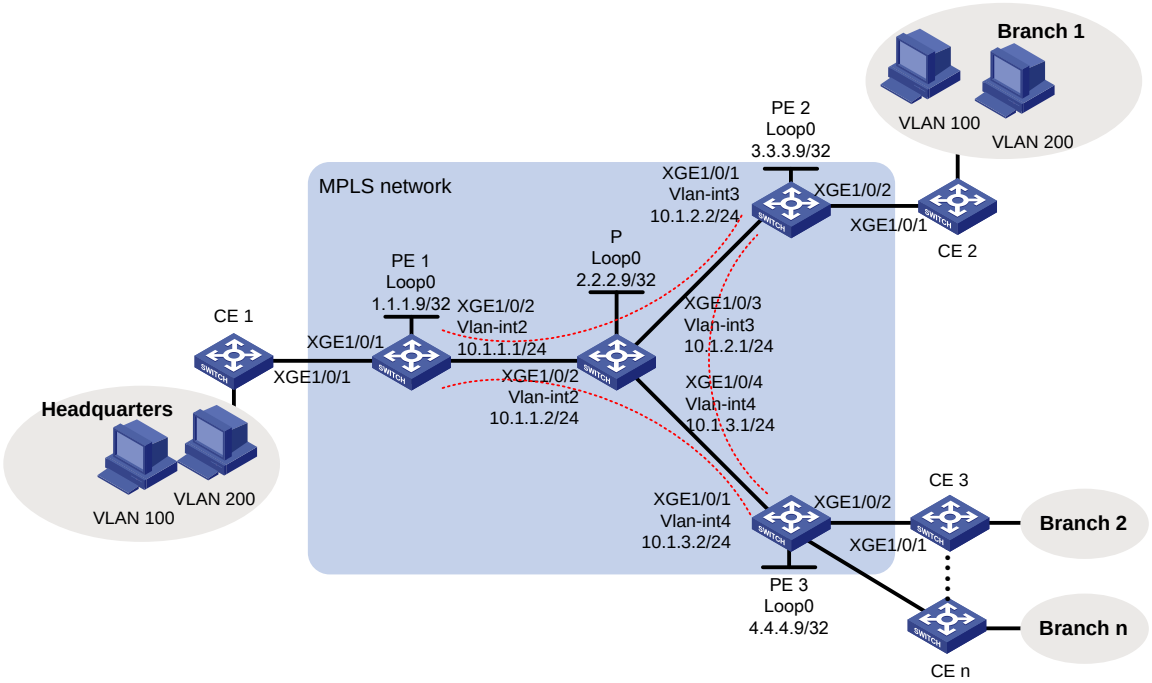
Example: Configuring full-mesh VPLS (BGP auto-discovery LDP signaling)

Network configuration

As shown in Figure 2, a company has multiple offices in different locations: headquarters and several branches. The company requires the provider to offer a Layer 2 VPN service that interconnects all offices at Layer 2, allowing them to share internal resources.

The company has many branches and will not expand further. To meet user requirements and reduce configuration and maintenance workload, use BGP auto-discovery LDP signaling to enable Layer 2 communication between all user sites.

Figure 2 Network diagram



Analysis

- Deploy MPLS on the backbone network and use LSP as the public tunnel.
- Configure and establish a BGP auto-discovery LDP signaling-based PW between any two PEs to achieve full mesh of PWs.
- Configure a service instance and corresponding match rules on the downlink port of each PE device to identify packets from the customer network that require a VPLS tunnel for transmission.
- To achieve VLAN isolation between sites, create VSIs **user_a** and **user_b** and bind them to VLAN 100 and VLAN 200, respectively.

Applicable hardware and software versions

Table 2 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx

Hardware	Software version
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported

Hardware	Software version
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices on the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  [PE1] interface loopback 0
  [PE1-LoopBack0] ip address 1.1.1.9 32
  [PE1-LoopBack0] quit
  ```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

  ```
  [PE1] vlan 2
  [PE1-vlan2] port ten-gigabitethernet 1/0/2
  [PE1-vlan2] quit
  ```

  # Create VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] ip address 10.1.1.1 24
  [PE1-Vlan-interface2] quit
  ```

  # Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

- Configure PE 2:

  # Configure a loopback interface address.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
```

  # Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

```
[PE2] vlan 3
[PE2-vlan3] port ten-gigabitethernet 1/0/1
[PE2-vlan3] quit
```

  # Create VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] quit
```

  # Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

- Configure PE 3:

  # Configure a loopback interface address.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 4.4.4.9 32
[PE3-LoopBack0] quit
```

  # Create VLAN 4 and add Ten-GigabitEthernet 1/0/1 to VLAN 4.

```
[PE3] vlan 4
[PE3-vlan4] port ten-gigabitethernet 1/0/1
[PE3-vlan4] quit
```

  # Create VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.1.3.2 24
[PE3-Vlan-interface4] quit
```

  # Configure OSPF on PE 3 for establishing LSPs.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
```

```
[PE3-ospf-1] quit
```

- Configure the P device:

  # Configure a loopback interface address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

  # Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[P] vlan 2
[P-vlan2] port ten-gigabitethernet 1/0/2
[P-vlan2] quit
```

  # Configure VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
```

  # Create VLAN 3 and add Ten-GigabitEthernet 3/0/1 to VLAN 3.

```
[P] vlan 3
[P-vlan3] port ten-gigabitethernet 1/0/3
[P-vlan3] quit
```

  # Configure VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] quit
```

  # Create VLAN 4 and add Ten-GigabitEthernet 1/0/4 to VLAN 4.

```
[P] vlan 4
[P-vlan4] port ten-gigabitethernet 1/0/4
[P-vlan4] quit
```

  # Configure VLAN-interface 4.

```
[P] interface vlan-interface 4
[P-Vlan-interface4] ip address 10.1.3.1 24
[P-Vlan-interface4] quit
```

  # Configure OSPF on the P device for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring basic MPLS and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

```
[PE1] mpls lsr-id 1.1.1.9
```

  # Enable LDP globally.

```
[PE1] mpls ldp
```

```
[PE1-ldp] quit
```

Enable MPLS and LDP VLAN-interface 2.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] mpls enable
[PE1-Vlan-interface2] mpls ldp enable
[PE1-Vlan-interface2] quit
```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable LDP globally.

  ```
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] mpls ldp enable
  [PE2-Vlan-interface3] quit
  ```

- Configure PE 3:

  # Configure an LSR ID.

  ```
  [PE3] mpls lsr-id 4.4.4.9
  ```

  # Enable LDP globally.

  ```
  [PE3] mpls ldp
  [PE3-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 4.

  ```
  [PE3] interface vlan-interface 4
  [PE3-Vlan-interface4] mpls enable
  [PE3-Vlan-interface4] mpls ldp enable
  [PE3-Vlan-interface4] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

  ```
  [P] mpls ldp
  [P-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [P] interface vlan-interface 2
  [P-Vlan-interface2] mpls enable
  [P-Vlan-interface2] mpls ldp enable
  [P-Vlan-interface2] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [P] interface vlan-interface 3
  [P-Vlan-interface3] mpls enable
  [P-Vlan-interface3] mpls ldp enable
  [P-Vlan-interface3] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 4.

  ```
  [P] interface vlan-interface 4
  [P-Vlan-interface4] mpls enable
  ```

```
[P-Vlan-interface4] mpls ldp enable
[P-Vlan-interface4] quit
```

Creating a VSI and configuring BGP auto-discovery LDP PWs

- Configure PE 1:

  # Create an IBGP connection to PE 2 and PE 3, respectively.

```
[PE1] bgp 100
[PE1-bgp-default] peer 3.3.3.9 as-number 100
[PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp-default] peer 4.4.4.9 as-number 100
[PE1-bgp-default] peer 4.4.4.9 connect-interface loopback 0
```

  # Enable BGP to advertise L2VPN information.

```
[PE1-bgp-default] address-family l2vpn
[PE1-bgp-default-l2vpn] peer 3.3.3.9 enable
[PE1-bgp-default-l2vpn] peer 4.4.4.9 enable
[PE1-bgp-default-l2vpn] quit
[PE1-bgp-default] quit
```

  # Enable MPLS L2VPN globally.

```
[PE1] l2vpn enable
```

  # Create VSI **user_a** that automatically discovers neighbors through BGP.

```
[PE1] vsi user_a
[PE1-vsi-user_a] auto-discovery bgp
```

  # Configure an RD and route target for the auto-discovery VSI.

```
[PE1-vsi-user_a-auto] route-distinguisher 100:1
[PE1-vsi-user_a-auto] vpn-target 111:1
```

  # Use LDP to create a PW to an automatically discovered remote PE.

```
[PE1-vsi-user_a-auto] signaling-protocol ldp
```

  # Configure a VPLS ID for the VSI.

```
[PE1-vsi-user_a-auto-ldp] vpls-id 100:100
[PE1-vsi-user_a-auto-ldp] quit
[PE1-vsi-user_a-auto] quit
[PE1-vsi-user_a] quit
```

  # Create VSI **user_b** that automatically discovers neighbors through BGP.

```
[PE1] vsi user_b
[PE1-vsi-user_b] auto-discovery bgp
```

  # Configure an RD and route target for the auto-discovery VSI.

```
[PE1-vsi-user_b-auto] route-distinguisher 200:1
[PE1-vsi-user_b-auto] vpn-target 222:1
```

  # Use LDP to create a PW to an automatically discovered remote PE.

```
[PE1-vsi-user_b-auto] signaling-protocol ldp
```

  # Configure a VPLS ID for the VSI.

```
[PE1-vsi-user_b-auto-ldp] vpls-id 200:200
[PE1-vsi-user_b-auto-ldp] quit
[PE1-vsi-user_b-auto] quit
[PE1-vsi-user_b] quit
```

- Configure PE 2:

  # Create an IBGP connection to PE 1 and PE 3, respectively.

```
[PE2] bgp 100
[PE2-bgp-default] peer 1.1.1.9 as-number 100
[PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp-default] peer 4.4.4.9 as-number 100
[PE2-bgp-default] peer 4.4.4.9 connect-interface loopback 0
```

Enable BGP to advertise L2VPN information.

```
[PE2-bgp-default] address-family l2vpn
[PE2-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE2-bgp-default-l2vpn] peer 4.4.4.9 enable
[PE2-bgp-default-l2vpn] quit
[PE2-bgp-default] quit
```

Enable MPLS L2VPN globally.

```
[PE2] l2vpn enable
```

Create **VSI user_a** that automatically discovers neighbors through BGP.

```
[PE2] vsi user_a
[PE2-vsi-user_a] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE2-vsi-user_a-auto] route-distinguisher 100:1
[PE2-vsi-user_a-auto] vpn-target 111:1
```

Use LDP to create a PW to an automatically discovered remote PE.

```
[PE2-vsi-user_a-auto] signaling-protocol ldp
```

Configure a VPLS ID for the VSI.

```
[PE2-vsi-user_a-auto-ldp] vpls-id 100:100
[PE2-vsi-user_a-auto-ldp] quit
[PE2-vsi-user_a-auto] quit
[PE2-vsi-user_a] quit
```

Create VSI **user_b** that automatically discovers neighbors through BGP.

```
[PE2] vsi user_b
[PE2-vsi-user_b] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE2-vsi-user_b-auto] route-distinguisher 200:1
[PE2-vsi-user_b-auto] vpn-target 222:1
```

Use LDP to create a PW to an automatically discovered remote PE.

```
[PE2-vsi-user_b-auto] signaling-protocol ldp
```

Configure a VPLS ID for the VSI.

```
[PE2-vsi-user_b-auto-ldp] vpls-id 200:200
[PE2-vsi-user_b-auto-ldp] quit
[PE2-vsi-user_b-auto] quit
[PE2-vsi-user_b] quit
```

- Configure PE 3:

  # Create an IBGP connection to PE 1 and PE 2, respectively.

  ```
  [PE3] bgp 100
  [PE3-bgp-default] peer 1.1.1.9 as-number 100
  [PE3-bgp-default] peer 1.1.1.9 connect-interface loopback 0
  [PE3-bgp-default] peer 3.3.3.9 as-number 100
  [PE3-bgp-default] peer 3.3.3.9 connect-interface loopback 0
  ```

  # Enable BGP to advertise L2VPN information.

```
[PE3-bgp-default] address-family l2vpn
[PE3-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE3-bgp-default-l2vpn] peer 3.3.3.9 enable
[PE3-bgp-default-l2vpn] quit
[PE3-bgp-default] quit
```

Enable MPLS L2VPN globally.

```
[PE3] l2vpn enable
```

Create VSI **user_a** that automatically discovers neighbors through BGP.

```
[PE3] vsi user_a
[PE3-vsi-user_a] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE3-vsi-user_a-auto] route-distinguisher 100:1
[PE3-vsi-user_a-auto] vpn-target 111:1
```

Use LDP to create a PW to an automatically discovered remote PE.

```
[PE3-vsi-user_a-auto] signaling-protocol ldp
```

Configure a VPLS ID for the VSI.

```
[PE3-vsi-user_a-auto-ldp] vpls-id 100:100
[PE3-vsi-user_a-auto-ldp] quit
[PE3-vsi-user_a-auto] quit
[PE3-vsi-user_a] quit
```

Create VSI **user_b** that automatically discovers neighbors through BGP.

```
[PE3] vsi user_b
[PE3-vsi-user_b] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE3-vsi-user_b-auto] route-distinguisher 200:1
[PE3-vsi-user_b-auto] vpn-target 222:1
```

Use LDP to create a PW to an automatically discovered remote PE.

```
[PE3-vsi-user_b-auto] signaling-protocol ldp
```

Configure a VPLS ID for the VSI.

```
[PE3-vsi-user_b-auto-ldp] vpls-id 200:200
[PE3-vsi-user_b-auto-ldp] quit
[PE3-vsi-user_b-auto] quit
[PE3-vsi-user_b] quit
```

Configuring service instances for data from different VLANs and bind them to different VSIs

- Configure PE 1:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE1] interface ten-gigabitethernet 1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] xconnect vsi user_a
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] xconnect vsi user_b
  ```

```
[PE1-Ten-GigabitEthernet1/0/1-srv200] quit
[PE1-Ten-GigabitEthernet1/0/1] quit
```

- Configure PE 2:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

```
[PE2] interface ten-gigabitethernet 1/0/2
[PE2-Ten-GigabitEthernet1/0/2] service-instance 100
[PE2-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
[PE2-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
[PE2-Ten-GigabitEthernet1/0/2-srv100] quit
```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

```
[PE2-Ten-GigabitEthernet1/0/2] service-instance 200
[PE2-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
[PE2-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
[PE2-Ten-GigabitEthernet1/0/2-srv200] quit
[PE2-Ten-GigabitEthernet1/0/2] quit
```

- Configure PE 3:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

```
[PE3] interface ten-gigabitethernet 1/0/2
[PE3-Ten-GigabitEthernet1/0/2] service-instance 100
[PE3-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
[PE3-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
[PE3-Ten-GigabitEthernet1/0/2-srv100] quit
```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

```
[PE3-Ten-GigabitEthernet1/0/2] service-instance 200
[PE3-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
[PE3-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
[PE3-Ten-GigabitEthernet1/0/2-srv200] quit
[PE3-Ten-GigabitEthernet1/0/2] quit
```

  # Configure interfaces on other CEs in the same way Ten-GigabitEthernet1/0/2 is configured.

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the site to pass through. The following uses CE 1 as an example. Configure other CEs in the same way CE1 is configured.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] vlan 200
[CE1-vlan200] quit
[CE1] interface ten-gigabitethernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Verifying the configuration

Verifying the public network LSPs

Execute the **display mpls ldp lsp** command to verify that the LSPs have been established.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal
Statistics:
  FECs: 4      Ingress LSPs: 3     Transit LSPs: 3     Egress LSPs: 1

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1148(L)
                   -/1151(L)
                   -/1151(L)
2.2.2.9/32         -/3             10.1.1.2        Vlan2
                   1151/3          10.1.1.2        Vlan2
                   -/1150(L)
                   -/1150(L)
3.3.3.9/32         -/1146          10.1.1.2        Vlan2
                   1149/1146       10.1.1.2        Vlan2
                   -/1149(L)
                   -/3(L)
4.4.4.9/32         -/1147          10.1.1.2        Vlan2
                   1150/1147       10.1.1.2        Vlan2
                   -/3(L)
                   -/1149(L)
```

Verifying PW status

Execute the **display l2vpn pw** command on each PE. The output shows that a PW has been established and in up state.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 4
4 up, 0 blocked, 0 down, 0 defect, 0 idle, 0 duplicate

VSI Name: user_a
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
3.3.3.9         -                 131195/131195   LDP     M     64       Up
4.4.4.9         -                 131194/1145     LDP     M     65       Up

VSI Name: user_b
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
4.4.4.9         -                 131193/1143     LDP     M     64       Up
3.3.3.9         -                 131192/131192   LDP     M     65       Up
```

Use ping to identify whether hosts within the same VLAN but at different sites can reach each other. If the ping operation succeeds, the VPLS is created successfully.

Configuration files

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 100:100
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 200:200
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
```

```
  xconnect vsi user_b
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 100
 peer 4.4.4.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 3.3.3.9 enable
  peer 4.4.4.9 enable
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 100:100
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 200:200
#
interface LoopBack0
```

```
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 100
 peer 4.4.4.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 1.1.1.9 enable
  peer 4.4.4.9 enable
#
```

- PE 3

```
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
#
 mpls lsr-id 4.4.4.9
#
vlan 4
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
```

```
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 100:100
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol ldp
   vpls-id 200:200
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface4
 ip address 10.1.3.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 1.1.1.9 enable
  peer 3.3.3.9 enable
#
```

- P

```
#
ospf 1
 area 0.0.0.0
```

```
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 4
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface4
 ip address 10.1.3.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 4
#
```

- CE 1 through CE n

```
#
vlan 100
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 200
#
```

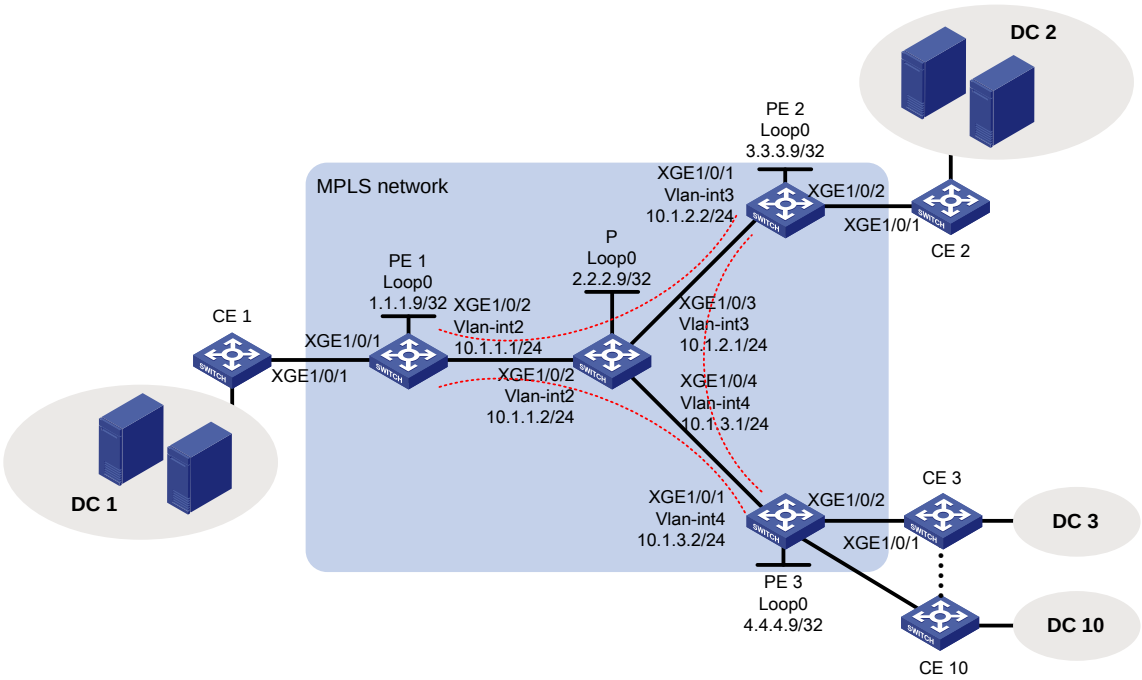
Example: Configuring full-mesh VPLS (BGP)

Network configuration

As shown in Figure 3, a company has 10 data centers located in different geographical areas and plans to add 15 more data centers. The company requires the provider to offer Layer 2 VPN services, enabling all data centers to interconnect at Layer 2 and share data resources.

The company has many data center sites and requires large-scale expansion. To meet user requirements, deploy BGP-based VPLS services.

Figure 3 Network diagram



Analysis

- Deploy MPLS on the backbone network and use LSP as the public tunnel.
- Deploy BGP-based VPLS service on PEs and configure label blocks to meet expansion requirements.
- To achieve VLAN isolation between sites, create VSIs **user_a** and **user_b** and bind them to VLAN 100 and VLAN 200, respectively.

Applicable hardware and software versions

Table 3 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI	Unsupported

Hardware	Software version
S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring IGP on the MPLS backbone network to enable communication between PEs and P devices on the backbone network

- Configure PE 1:

  # Configure a loopback interface address.

  ```
  <PE1> system-view
  ```

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
```

Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[PE1] vlan 2
[PE1-vlan2] port ten-gigabitethernet 1/0/2
[PE1-vlan2] quit
```

Create VLAN-interface 2.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] quit
```

Configure OSPF on PE 1 for establishing LSPs.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

- Configure PE 2:

Configure a loopback interface address.

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
```

Create VLAN 3 and add Ten-GigabitEthernet 1/0/1 to VLAN 3.

```
[PE2] vlan 3
[PE2-vlan3] port ten-gigabitethernet 1/0/1
[PE2-vlan3] quit
```

Create VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.1.2.2 24
[PE2-Vlan-interface3] quit
```

Configure OSPF on PE 2 for establishing LSPs.

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

- Configure PE 3:

Configure a loopback interface address.

```
<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 4.4.4.9 32
[PE3-LoopBack0] quit
```

Create VLAN 4 and add Ten-GigabitEthernet 1/0/1 to VLAN 4.

```
[PE3] vlan 4
```

```
[PE3-vlan4] port ten-gigabitethernet 1/0/1
[PE3-vlan4] quit
```

Create VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.1.3.2 24
[PE3-Vlan-interface4] quit
```

Configure OSPF on PE 3 for establishing LSPs.

```
[PE3] ospf
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

- Configure the P device:

Configure a loopback interface address.

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
```

Create VLAN 2 and add Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[P] vlan 2
[P-vlan2] port ten-gigabitethernet 1/0/2
[P-vlan2] quit
```

Configure VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] ip address 10.1.1.2 24
[P-Vlan-interface2] quit
```

Create VLAN 3 and add Ten-GigabitEthernet 3/0/1 to VLAN 3.

```
[P] vlan 3
[P-vlan3] port ten-gigabitethernet 1/0/3
[P-vlan3] quit
```

Configure VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 10.1.2.1 24
[P-Vlan-interface3] quit
```

Create VLAN 4 and add Ten-GigabitEthernet 1/0/4 to VLAN 4.

```
[P] vlan 4
[P-vlan4] port ten-gigabitethernet 1/0/4
[P-vlan4] quit
```

Configure VLAN-interface 4.

```
[P] interface vlan-interface 4
[P-Vlan-interface4] ip address 10.1.3.1 24
[P-Vlan-interface4] quit
```

Configure OSPF on the P device for establishing LSPs.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

Configuring basic MPLS and MPLS LDP on the MPLS backbone network to establish LDP LSPs

- Configure PE 1:

  # Configure an LSR ID.

  ```
  [PE1] mpls lsr-id 1.1.1.9
  ```

  # Enable LDP globally.

  ```
  [PE1] mpls ldp
  [PE1-ldp] quit
  ```

  # Enable MPLS and LDP VLAN-interface 2.

  ```
  [PE1] interface vlan-interface 2
  [PE1-Vlan-interface2] mpls enable
  [PE1-Vlan-interface2] mpls ldp enable
  [PE1-Vlan-interface2] quit
  ```

- Configure PE 2:

  # Configure an LSR ID.

  ```
  [PE2] mpls lsr-id 3.3.3.9
  ```

  # Enable LDP globally.

  ```
  [PE2] mpls ldp
  [PE2-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 3.

  ```
  [PE2] interface vlan-interface 3
  [PE2-Vlan-interface3] mpls enable
  [PE2-Vlan-interface3] mpls ldp enable
  [PE2-Vlan-interface3] quit
  ```

- Configure PE 3:

  # Configure an LSR ID.

  ```
  [PE3] mpls lsr-id 4.4.4.9
  ```

  # Enable LDP globally.

  ```
  [PE3] mpls ldp
  [PE3-ldp] quit
  ```

  # Enable MPLS and LDP on VLAN-interface 4.

  ```
  [PE3] interface vlan-interface 4
  [PE3-Vlan-interface4] mpls enable
  [PE3-Vlan-interface4] mpls ldp enable
  [PE3-Vlan-interface4] quit
  ```

- Configure the P device:

  # Configure an LSR ID.

  ```
  [P] mpls lsr-id 2.2.2.9
  ```

  # Enable LDP globally.

  ```
  [P] mpls ldp
  [P-ldp] quit
  ```

Enable MPLS and LDP VLAN-interface 2.

```
[P] interface vlan-interface 2
[P-Vlan-interface2] mpls enable
[P-Vlan-interface2] mpls ldp enable
[P-Vlan-interface2] quit
```

Enable MPLS and LDP on VLAN-interface 3.

```
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls enable
[P-Vlan-interface3] mpls ldp enable
[P-Vlan-interface3] quit
```

Enable MPLS and LDP on VLAN-interface 4.

```
[P] interface vlan-interface 4
[P-Vlan-interface4] mpls enable
[P-Vlan-interface4] mpls ldp enable
[P-Vlan-interface4] quit
```

Creating a VSI and configuring BGP PWs

- Configure PE 1:

  # Create an IBGP connection to PE 2 and PE 3, respectively.

  ```
  [PE1] bgp 100
  [PE1-bgp-default] peer 3.3.3.9 as-number 100
  [PE1-bgp-default] peer 3.3.3.9 connect-interface loopback 0
  [PE1-bgp-default] peer 4.4.4.9 as-number 100
  [PE1-bgp-default] peer 4.4.4.9 connect-interface loopback 0
  ```

  # Enable BGP to advertise L2VPN information.

  ```
  [PE1-bgp-default] address-family l2vpn
  [PE1-bgp-default-l2vpn] peer 3.3.3.9 enable
  [PE1-bgp-default-l2vpn] peer 4.4.4.9 enable
  [PE1-bgp-default-l2vpn] quit
  [PE1-bgp-default] quit
  ```

  # Enable MPLS L2VPN globally.

  ```
  [PE1] l2vpn enable
  ```

  # Create VSI **user_a** that automatically discovers neighbors through BGP.

  ```
  [PE1] vsi user_a
  [PE1-vsi-user_a] auto-discovery bgp
  ```

  # Configure an RD and route target for the auto-discovery VSI.

  ```
  [PE1-vsi-user_a-auto] route-distinguisher 100:1
  [PE1-vsi-user_a-auto] vpn-target 111:1
  ```

  # Use BGP to create a PW to an automatically discovered remote PE.

  ```
  [PE1-vsi-user_a-auto] signaling-protocol bgp
  ```

  # Configure the site number for PE 1 in this instance (using 1 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

  ```
  [PE1-vsi-user_a-auto-bgp] site 1 range 25
  [PE1-vsi-user_a-auto-bgp] quit
  [PE1-vsi-user_a-auto] quit
  [PE1-vsi-user_a] quit
  ```

  # Create VSI **user_b** that automatically discovers neighbors through BGP.

```
[PE1] vsi user_b
[PE1-vsi-user_b] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE1-vsi-user_b-auto] route-distinguisher 200:1
[PE1-vsi-user_b-auto] vpn-target 222:1
```

Use BGP to create a PW to an automatically discovered remote PE.

```
[PE1-vsi-user_b-auto] signaling-protocol bgp
```

Configure the site number for PE 1 in this instance (using 1 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

```
[PE1-vsi-user_b-auto-bgp] site 1 range 25
[PE1-vsi-user_b-auto-bgp] quit
[PE1-vsi-user_b-auto] quit
[PE1-vsi-user_b] quit
```

- Configure PE 2:

Create an IBGP connection to PE 1 and PE 3, respectively.

```
[PE2] bgp 100
[PE2-bgp-default] peer 1.1.1.9 as-number 100
[PE2-bgp-default] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp-default] peer 4.4.4.9 as-number 100
[PE2-bgp-default] peer 4.4.4.9 connect-interface loopback 0
```

Enable BGP to advertise L2VPN information.

```
[PE2-bgp-default] address-family l2vpn
[PE2-bgp-default-l2vpn] peer 1.1.1.9 enable
[PE2-bgp-default-l2vpn] peer 4.4.4.9 enable
[PE2-bgp-default-l2vpn] quit
[PE2-bgp-default] quit
```

Enable MPLS L2VPN globally.

```
[PE2] l2vpn enable
```

Create VSI **user_a** that automatically discovers neighbors through BGP.

```
[PE2] vsi user_a
[PE2-vsi-user_a] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE2-vsi-user_a-auto] route-distinguisher 100:1
[PE2-vsi-user_a-auto] vpn-target 111:1
```

Use BGP to create a PW to an automatically discovered remote PE.

```
[PE2-vsi-user_a-auto] signaling-protocol bgp
```

Configure the site number for PE 2 in this instance (using 2 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

```
[PE2-vsi-user_a-auto-bgp] site 2 range 25
[PE2-vsi-user_a-auto-bgp] quit
[PE2-vsi-user_a-auto] quit
[PE2-vsi-user_a] quit
```

Create VSI **user_b** that automatically discovers neighbors through BGP.

```
[PE2] vsi user_b
[PE2-vsi-user_b] auto-discovery bgp
```

Configure an RD and route target for the auto-discovery VSI.

```
[PE2-vsi-user_b-auto] route-distinguisher 200:1
[PE2-vsi-user_b-auto] vpn-target 222:1
```

Use BGP to create a PW to an automatically discovered remote PE.

```
[PE2-vsi-user_b-auto] signaling-protocol bgp
```

Configure the site number for PE 2 in this instance (using 2 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

```
[PE2-vsi-user_b-auto-bgp] site 2 range 25
[PE2-vsi-user_b-auto-bgp] quit
[PE2-vsi-user_b-auto] quit
[PE2-vsi-user_b] quit
```

- Configure PE 3:

  # Create an IBGP connection to PE 1 and PE 2, respectively.

  ```
  [PE3] bgp 100
  [PE3-bgp-default] peer 1.1.1.9 as-number 100
  [PE3-bgp-default] peer 1.1.1.9 connect-interface loopback 0
  [PE3-bgp-default] peer 3.3.3.9 as-number 100
  [PE3-bgp-default] peer 3.3.3.9 connect-interface loopback 0
  ```

  # Enable BGP to advertise L2VPN information.

  ```
  [PE3-bgp-default] address-family l2vpn
  [PE3-bgp-default-l2vpn] peer 1.1.1.9 enable
  [PE3-bgp-default-l2vpn] peer 3.3.3.9 enable
  [PE3-bgp-default-l2vpn] quit
  [PE3-bgp-default] quit
  ```

  # Enable MPLS L2VPN globally.

  ```
  [PE3] l2vpn enable
  ```

  # Create VSI **user_a** that automatically discovers neighbors through BGP.

  ```
  [PE3] vsi user_a
  [PE3-vsi-user_a] auto-discovery bgp
  ```

  # Configure an RD and route target for the auto-discovery VSI.

  ```
  [PE3-vsi-user_a-auto] route-distinguisher 100:1
  [PE3-vsi-user_a-auto] vpn-target 111:1
  ```

  # Use BGP to create a PW to an automatically discovered remote PE.

  ```
  [PE3-vsi-user_a-auto] signaling-protocol bgp
  ```

  # Configure the site number for PE 3 in this instance (using 3 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

  ```
  [PE3-vsi-user_a-auto-bgp] site 3 range 25
  [PE3-vsi-user_a-auto-bgp] quit
  [PE3-vsi-user_a-auto] quit
  [PE3-vsi-user_a] quit
  ```

  # Create VSI **user_b** that automatically discovers neighbors through BGP.

  ```
  [PE3] vsi user_b
  [PE3-vsi-user_b] auto-discovery bgp
  ```

  # Configure an RD and route target for the auto-discovery VSI.

  ```
  [PE3-vsi-user_b-auto] route-distinguisher 200:1
  [PE3-vsi-user_b-auto] vpn-target 222:1
  ```

  # Use BGP to create a PW to an automatically discovered remote PE.

```
[PE3-vsi-user_b-auto] signaling-protocol bgp
```

Configure the site number for PE 3 in this instance (using 3 as an example), and the number of PEs that can establish connections in this instance (the value should be 25, because there are 10 sites in the network and 15 more will be added).

```
[PE3-vsi-user_b-auto-bgp] site 3 range 25
[PE3-vsi-user_b-auto-bgp] quit
[PE3-vsi-user_b-auto] quit
[PE3-vsi-user_b] quit
```

Configuring service instances for data from different VLANs and bind them to different VSIs

- Configure PE 1:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE1] interface ten-gigabitethernet 1/0/1
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] encapsulation s-vid 100
  [PE1-Ten-GigabitEthernet1/0/1-srv100] xconnect vsi user_a
  [PE1-Ten-GigabitEthernet1/0/1-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE1-Ten-GigabitEthernet1/0/1] service-instance 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] encapsulation s-vid 200
  [PE1-Ten-GigabitEthernet1/0/1-srv200] xconnect vsi user_b
  [PE1-Ten-GigabitEthernet1/0/1-srv200] quit
  [PE1-Ten-GigabitEthernet1/0/1] quit
  ```

- Configure PE 2:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 100, and bind it to VSI instance **user_a**.

  ```
  [PE2] interface ten-gigabitethernet 1/0/2
  [PE2-Ten-GigabitEthernet1/0/2] service-instance 100
  [PE2-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
  [PE2-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
  [PE2-Ten-GigabitEthernet1/0/2-srv100] quit
  ```

  # Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

  ```
  [PE2-Ten-GigabitEthernet1/0/2] service-instance 200
  [PE2-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
  [PE2-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
  [PE2-Ten-GigabitEthernet1/0/2-srv200] quit
  [PE2-Ten-GigabitEthernet1/0/2] quit
  ```

- Configure PE 3:

  # Create service instance 100 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 100, and bind it to VSI **user_a**.

  ```
  [PE3] interface ten-gigabitethernet 1/0/2
  [PE3-Ten-GigabitEthernet1/0/2] service-instance 100
  [PE3-Ten-GigabitEthernet1/0/2-srv100] encapsulation s-vid 100
  [PE3-Ten-GigabitEthernet1/0/2-srv100] xconnect vsi user_a
  [PE3-Ten-GigabitEthernet1/0/2-srv100] quit
  ```

Create service instance 200 on Ten-GigabitEthernet 1/0/2 to match packets from VLAN 200, and bind it to VSI instance **user_b**.

```
[PE3-Ten-GigabitEthernet1/0/2] service-instance 200
[PE3-Ten-GigabitEthernet1/0/2-srv200] encapsulation s-vid 200
[PE3-Ten-GigabitEthernet1/0/2-srv200] xconnect vsi user_b
[PE3-Ten-GigabitEthernet1/0/2-srv200] quit
[PE3-Ten-GigabitEthernet1/0/2] quit
```

Configure interfaces on other CEs in the same way Ten-GigabitEthernet1/0/2 is configured.

Connecting CEs to PEs

Configure the uplink interface to the PE to allow tagged packets from the site to pass through. The following uses CE 1 as an example. Configure other CEs in the same way CE1 is configured.

```
<CE1> system-view
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] vlan 200
[CE1-vlan200] quit
[CE1] interface ten-gigabitethernet 1/0/1
[CE1-Ten-GigabitEthernet1/0/1] port link-type trunk
[CE1-Ten-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

Verifying the configuration

Verifying the public network LSPs

Execute the **display mpls ldp lsp** command to verify that the LSPs have been established.

```
[PE1] display mpls ldp lsp
Status Flags: * - stale, L - liberal
Statistics:
  FECs: 4      Ingress LSPs: 3     Transit LSPs: 3     Egress LSPs: 1

FEC                In/Out Label    Nexthop         OutInterface
1.1.1.9/32         3/-
                   -/1151(L)
2.2.2.9/32         -/3             10.1.1.2        Vlan2
                   1151/3          10.1.1.2        Vlan2
3.3.3.9/32         -/1150          10.1.1.2        Vlan2
                   1150/1150       10.1.1.2        Vlan2
4.4.4.9/32         -/1149          10.1.1.2        Vlan2
                   1149/1149       10.1.1.2        Vlan2
```

Verifying PW status

Execute the **display l2vpn pw** command on each PE. The output shows that a PW has been established and in up state.

```
[PE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 2, 2 up, 0 blocked, 0 down, 0 defect

VSI Name: user_a
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
```

```
3.3.3.9         2                131074/131073   BGP     M     257      Up
4.4.4.9         3                131075/131073   BGP     M     258      Up

VSI Name: user_b
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
3.3.3.9         2                131071/131070   BGP     M     257      Up
4.4.4.9         3                131072/131070   BGP     M     258      Up
```

Use ping to identify whether hosts within the same VLAN but at different sites can reach each other. If the ping operation succeeds, the VPLS is created successfully.

Configuration files

- PE 1

```
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
 mpls lsr-id 1.1.1.9
#
vlan 2
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol bgp
   site 1 range 25 default-offset 0
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol bgp
   site 1 range 25 default-offset 0
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
```

```
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
bgp 100
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 100
 peer 4.4.4.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 3.3.3.9 enable
  peer 4.4.4.9 enable
#
```

- PE 2

```
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
 mpls lsr-id 3.3.3.9
#
vlan 3
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol bgp
   site 2 range 25 default-offset 0
```

```
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol bgp
   site 2 range 25 default-offset 0
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface3
 ip address 10.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 4.4.4.9 as-number 100
 peer 4.4.4.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 1.1.1.9 enable
  peer 4.4.4.9 enable
#
```

- PE 3

```
#
ospf 1
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
#
 mpls lsr-id 4.4.4.9
```

```
#
vlan 4
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 auto-discovery bgp
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
  signaling-protocol bgp
   site 3 range 25 default-offset 0
#
vsi user_b
 auto-discovery bgp
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
  signaling-protocol bgp
   site 3 range 25 default-offset 0
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface4
 ip address 10.1.3.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 100
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 200
  encapsulation s-vid 200
  xconnect vsi user_b
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
 peer 3.3.3.9 as-number 100
```

```
 peer 3.3.3.9 connect-interface LoopBack0
 #
 address-family l2vpn
  peer 1.1.1.9 enable
  peer 3.3.3.9 enable
#
```

- P

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
 mpls lsr-id 2.2.2.9
#
vlan 2 to 4
#
mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface3
 ip address 10.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface4
 ip address 10.1.3.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 3
#
interface Ten-GigabitEthernet1/0/4
```

```
 port link-mode bridge
 port access vlan 4
#
```

- CE 1 through CE 10

```
#
vlan 100
#
vlan 200
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 100 200
#
```

Example: Configuring H-VPLS (LSP access)

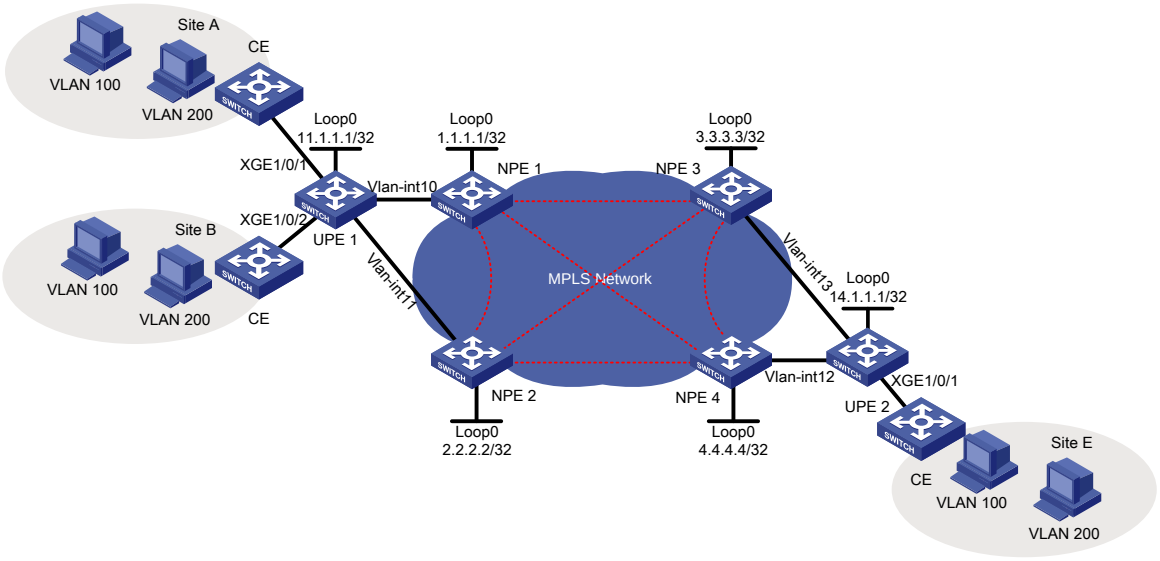
Network configuration

A provider provides VPLS service, with numerous users in various locations. To simplify the network structure and reduce device load and maintenance workload, deploy H-VPLS on the network.

As shown in Figure 4, make sure the following requirements are met:

- Branches at different locations connect to the carrier MPLS network through UPEs that support MPLS L2VPN.
- NPEs connect to the UPEs by using the LSP access mode.
- The UPEs are dual homed to two NPEs for increased reliability.

Figure 4 Network diagram



Device	Interface	IP address	Device	Interface	IP address
UPE 1	Loop0	11.1.1.1/32	UPE 2	Loop0	14.1.1.1/32
	Vlan-int10	11.1.2.1/24		Vlan-int12	20.1.1.1/24
	Vlan-int11	11.1.3.1/24		Vlan-int13	20.1.2.1/24
NPE 1	Loop0	1.1.1.1/32	NPE 3	Loop0	3.3.3.3/32
	Vlan-int10	11.1.2.2/24		Vlan-int13	20.1.2.2/24
NPE 2	Loop0	2.2.2.2/32	NPE 4	Loop0	4.4.4.4/32
	Vlan-int11	11.1.3.2/24		Vlan-int12	20.1.1.2/24

Analysis

- To negotiate the inner labels, establish remote LDP peer relationships between the UPEs and all connected NPEs, as well as between any two NPEs.
- On the UPEs, set up primary/backup peers to determine the primary and backup status of the links.
- Configure a service instance and corresponding match rules on the downlink port of each UPE identify packets from the customer network that require a VPLS tunnel for transmission.
- To achieve VLAN isolation between sites, create VSIs **user_a** and **user_b** and bind them to VLAN 100 and VLAN 200, respectively.

Applicable hardware and software versions

Table 4 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series	Release 6628Pxx series

Hardware	Software version
S6520-SI series	
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series	Unsupported

Hardware	Software version
MS4320V3 series MS4300V2 series MS4320 series MS4200 series	
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring basic network settings

1. Create interfaces for UPE and NPE devices as shown in Figure 4 and configure IP addresses for them. (Details not shown.)
2. Configure IGP on the MPLS backbone network to ensure that all interfaces on the NPEs and UPEs are reachable to each other. (Details not shown.)
3. Configure basic MPLS and MPLS LDP on the backbone network to establish LDP LSPs. (Details not shown.)
4. Configure interfaces on each CE that connect to UPEs as a trunk port and permit packets from VLAN 100 and VLAN 200 to pass through with tags. (Details not shown.)

Configuring UPE 1

Configure basic MPLS.

```
<UPE1> system-view
[UPE1] mpls lsr-id 11.1.1.1
[UPE1] mpls ldp
[UPE1-ldp] quit
```

Configure basic MPLS capability on the interface connected with NPE 1.

```
[UPE1] interface vlan-interface 10
[UPE1-Vlan-interface10] mpls enable
[UPE1-Vlan-interface10] mpls ldp enable
[UPE1-Vlan-interface10] quit
```

Configure basic MPLS capability on the interface connected with NPE 2.

```
[UPE1] interface vlan-interface 11
[UPE1-Vlan-interface11] mpls enable
[UPE1-Vlan-interface11] mpls ldp enable
[UPE1-Vlan-interface11] quit
```

Enable MPLS L2VPN.

```
[UPE1] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[UPE1] vsi user_a
[UPE1-vsi-user_a] pwsignaling ldp
```

Specify the switchover mode and set the wait time to 120 seconds for the switchover.

```
[UPE1-vsi-user_a-ldp] revertive wtr 120
```

Configure a static PW between UPE 1 and NPE 1, and a backup static PW between UPE 1 and NPE 2.

```
[UPE1-vsi-user_a-ldp] peer 1.1.1.1 pw-id 500
[UPE1-vsi-user_a-ldp-1.1.1.1-500] backup-peer 2.2.2.2 pw-id 500
[UPE1-vsi-user_a-ldp-1.1.1.1-500-backup] quit
[UPE1-vsi-user_a-ldp-1.1.1.1-500] quit
[UPE1-vsi-user_a-ldp] quit
[UPE1-vsi-user_a] quit
```

Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[UPE1] vsi user_b
[UPE1-vsi-user_b] pwsignaling ldp
```

Specify the switchover mode and set the wait time to 120 seconds for the switchover.

```
[UPE1-vsi-user_b-ldp] revertive wtr 120
```

Configure a static PW between UPE 1 and NPE 1, and a backup static PW between UPE 1 and NPE 2.

```
[UPE1-vsi-user_b-ldp] peer 1.1.1.1 pw-id 600
[UPE1-vsi-user_b-ldp-1.1.1.1-600] backup-peer 2.2.2.2 pw-id 600
[UPE1-vsi-user_b-ldp-1.1.1.1-600-backup] quit
[UPE1-vsi-user_b-ldp-1.1.1.1-600] quit
[UPE1-vsi-user_b-ldp] quit
[UPE1-vsi-user_b] quit
```

Create service instance 1000 on Ten-GigabitEthernet 1/0/1 connected to Site A to match packets from VLAN 100, and bind it to VSI **user_a**.

```
[UPE1] interface ten-gigabitethernet 1/0/1
[UPE1-Ten-GigabitEthernet1/0/1] service-instance 1000
[UPE1-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[UPE1-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi user_a
[UPE1-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Create service instance 2000 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200, and bind it to VSI **user_b**.

```
[UPE1-Ten-GigabitEthernet1/0/1] service-instance 2000
[UPE1-Ten-GigabitEthernet1/0/1-srv2000] encapsulation s-vid 200
[UPE1-Ten-GigabitEthernet1/0/1-srv2000] xconnect vsi user_b
[UPE1-Ten-GigabitEthernet1/0/1-srv2000] quit
```

Create two service instances on Ten-GigabitEthernet1/0/2 connected to Site B to match packets from VALN 100 and VLAN 200, respectively, and bind VLAN 100 to VSI **user_a** and VLAN 200 to VSI **user_b**.

```
[UPE1] interface ten-gigabitethernet 1/0/2
[UPE1-Ten-GigabitEthernet1/0/2] service-instance 1000
[UPE1-Ten-GigabitEthernet1/0/2-srv1000] encapsulation s-vid 100
[UPE1-Ten-GigabitEthernet1/0/2-srv1000] xconnect vsi user_a
[UPE1-Ten-GigabitEthernet1/0/2-srv1000] quit
[UPE1-Ten-GigabitEthernet1/0/2] service-instance 2000
[UPE1-Ten-GigabitEthernet1/0/2-srv2000] encapsulation s-vid 200
```

```
[UPE1-Ten-GigabitEthernet1/0/2-srv2000] xconnect vsi user_b
[UPE1-Ten-GigabitEthernet1/0/2-srv2000] quit
```

Configuring NPE 1

Configure basic MPLS capability on the interface connected with UPE 1.

```
<NPE1> system-view
[NPE1] interface vlan-interface 10
[NPE1-Vlan-interface10] mpls enable
[NPE1-Vlan-interface10] mpls ldp enable
[NPE1-Vlan-interface10] quit
```

Enable MPLS L2VPN.

```
[NPE1] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[NPE1] vsi user_a
[NPE1-vsi-user_a] pwsignaling ldp
```

Specify UPE 1 as the peer.

```
[NPE1-vsi-user_a-ldp] peer 11.1.1.1 pw-id 500 no-split-horizon
[NPE1-vsi-user_a-ldp-11.1.1.1-500] quit
```

Specify NPE 2, NPE 3, and NPE 4 as the peer NPEs.

```
[NPE1-vsi-user_a-ldp] peer 2.2.2.2 pw-id 500
[NPE1-vsi-user_a-ldp-2.2.2.2-500] quit
[NPE1-vsi-user_a-ldp] peer 3.3.3.3 pw-id 500
[NPE1-vsi-user_a-ldp-3.3.3.3-500] quit
[NPE1-vsi-user_a-ldp] peer 4.4.4.4 pw-id 500
[NPE1-vsi-user_a-ldp-4.4.4.4-500] quit
[NPE1-vsi-user_a-ldp] quit
[NPE1-vsi-user_a] quit
```

Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[NPE1] vsi user_b
[NPE1-vsi-user_b] pwsignaling ldp
```

Specify UPE 1 as the peer.

```
[NPE1-vsi-user_b-ldp] peer 11.1.1.1 pw-id 600 no-split-horizon
[NPE1-vsi-user_b-ldp-11.1.1.1-500] quit
```

Specify NPE 2, NPE 3, and NPE 4 as the peer NPEs.

```
[NPE1-vsi-user_b-ldp] peer 2.2.2.2 pw-id 600
[NPE1-vsi-user_b-ldp-2.2.2.2-600] quit
[NPE1-vsi-user_b-ldp] peer 3.3.3.3 pw-id 600
[NPE1-vsi-user_b-ldp-3.3.3.3-600] quit
[NPE1-vsi-user_b-ldp] peer 4.4.4.4 pw-id 600
[NPE1-vsi-user_b-ldp-4.4.4.4-600] quit
[NPE1-vsi-user_b-ldp] quit
[NPE1-vsi-user_b] quit
```

Configuring NPE 2

The configuration for NPE 2 is similar to that for NPE 1 except that VLAN interfaces connected to UPE and the NPE peers for them are different. For more information about the configuration, see the configuration file.

Configuring UPE 2

Configure basic MPLS.

```
<UPE2> system-view
[UPE2] mpls lsr-id 14.1.1.1
[UPE2] mpls ldp
[UPE2-ldp] quit
```

Configure basic MPLS capability on the interface connected with NPE 3.

```
[UPE2] interface vlan-interface 13
[UPE2-Vlan-interface13] mpls enable
[UPE2-Vlan-interface13] mpls ldp enable
[UPE2-Vlan-interface13] quit
```

Configure basic MPLS capability on the interface connected with NPE 4.

```
[UPE2] interface vlan-interface 12
[UPE2-Vlan-interface12] mpls enable
[UPE2-Vlan-interface12] mpls ldp enable
[UPE2-Vlan-interface12] quit
```

Enable MPLS L2VPN.

```
[UPE2] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[UPE2] vsi user_a
[UPE2-vsi-user_a] pwsignaling ldp
```

Specify the switchover mode and set the wait time to 120 seconds for the switchover.

```
[UPE2-vsi-user_a-ldp] revertive wtr 120
```

Configure a static PW between UPE 2 and NPE 3, and a backup static PW between UPE 2 and NPE 4.

```
[UPE2-vsi-user_a-ldp] peer 3.3.3.3 pw-id 500
[UPE2-vsi-user_a-ldp-3.3.3.3-500] backup-peer 4.4.4.4 pw-id 500
[UPE2-vsi-user_a-ldp-3.3.3.3-500-backup] quit
[UPE2-vsi-user_a-ldp-3.3.3.3-500] quit
[UPE2-vsi-user_a-ldp] quit
[UPE2-vsi-user_a] quit
```

Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[UPE2] vsi user_b
[UPE2-vsi-user_b] pwsignaling ldp
```

Specify the switchover mode and set the wait time to 120 seconds for the switchover.

```
[UPE2-vsi-user_b-ldp] revertive wtr 120
```

Configure a static PW between UPE 2 and NPE 3, and a backup static PW between UPE 2 and NPE 4.

```
[UPE2-vsi-user_b-ldp] peer 3.3.3.3 pw-id 600
[UPE2-vsi-user_b-ldp-3.3.3.3-600] backup-peer 4.4.4.4 pw-id 600
[UPE2-vsi-user_b-ldp-3.3.3.3-600-backup] quit
[UPE2-vsi-user_b-ldp-3.3.3.3-600] quit
[UPE2-vsi-user_b-ldp] quit
[UPE2-vsi-user_b] quit
```

Create service instance 1000 on Ten-GigabitEthernet 1/0/1 connected to Site E to match packets from VLAN 100, and bind it to VSI **user_a**.

```
[UPE2] interface ten-gigabitethernet 1/0/1
[UPE2-Ten-GigabitEthernet1/0/1] service-instance 1000
[UPE2-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 100
[UPE2-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi user_a
[UPE2-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Create service instance 2000 on Ten-GigabitEthernet 1/0/1 to match packets from VLAN 200, and bind it to VSI **user_b**.

```
[UPE2-Ten-GigabitEthernet1/0/1] service-instance 2000
[UPE2-Ten-GigabitEthernet1/0/1-srv2000] encapsulation s-vid 200
[UPE2-Ten-GigabitEthernet1/0/1-srv2000] xconnect vsi user_b
[UPE2-Ten-GigabitEthernet1/0/1-srv2000] quit
```

Configuring NPE 3

Configure basic MPLS capability on the interface connected with UPE 2.

```
[NPE3] interface vlan-interface 13
[NPE3-Vlan-interface13] mpls enable
[NPE3-Vlan-interface13] mpls ldp enable
[NPE3-Vlan-interface13] quit
```

Configure MPLS L2VPN.

```
[NPE3] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[NPE3] vsi user_a
[NPE3-vsi-user_a] pwsignaling ldp
```

Specify UPE 2 as the peer.

```
[NPE3-vsi-user_a-ldp] peer 14.1.1.1 pw-id 500 no-split-horizon
[NPE3-vsi-user_a-ldp-14.1.1.1-500] quit
```

Specify NPE 1, NPE 2, and NPE 4 as the peer NPEs.

```
[NPE3-vsi-user_a-ldp] peer 1.1.1.1 pw-id 500
[NPE3-vsi-user_a-ldp-1.1.1.1-500] quit
[NPE3-vsi-user_a-ldp] peer 2.2.2.2 pw-id 500
[NPE3-vsi-user_a-ldp-2.2.2.2-500] quit
[NPE3-vsi-user_a-ldp] peer 4.4.4.4 pw-id 500
[NPE3-vsi-user_a-ldp-4.4.4.4-500] quit
[NPE3-vsi-user_a-ldp] quit
[NPE3-vsi-user_a] quit
```

Configure VSI **user_b** that uses LDP as the PW signaling protocol.

```
[NPE3] vsi user_b
[NPE3-vsi-user_b] pwsignaling ldp
```

Specify UPE 2 as the peer.

```
[NPE3-vsi-user_b-ldp] peer 14.1.1.1 pw-id 600 no-split-horizon
[NPE3-vsi-user_b-ldp-14.1.1.1-600] quit
```

Specify NPE 1, NPE 2, and NPE 4 as the peer NPEs.

```
[NPE3-vsi-user_b-ldp] peer 1.1.1.1 pw-id 600
[NPE3-vsi-user_b-ldp-1.1.1.1-600] quit
[NPE3-vsi-user_b-ldp] peer 2.2.2.2 pw-id 600
[NPE3-vsi-user_b-ldp-2.2.2.2-600] quit
[NPE3-vsi-user_b-ldp] peer 4.4.4.4 pw-id 600
```

```
[NPE3-vsi-user_b-ldp-4.4.4.4-600] quit
[NPE3-vsi-user_b-ldp] quit
[NPE3-vsi-user_b] quit
```

Configuring NPE 4

The configuration for NPE 4 is similar to that for NPE 3 except that VLAN interfaces connected to UPE and the NPE peers for them are different. For more information about the configuration, see the configuration file.

Verifying the configuration

Verify the state of PWs on each UPE and NPE. The following uses UPE 1 and NPE 1 as an example.

Use the **display l2vpn pw** command on UPE 1 to view the PW state.

```
[UPE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 4, 4 up, 0 blocked, 0 down, 0 defect

VSI Name: user_a
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
1.1.1.1         500               131199/131199   LDP     M     256      Up
2.2.2.2         500               131198/131199   LDP     B     257      Blocked

VSI Name: user_b
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
1.1.1.1         600               131195/131195   LDP     M     256      Up
2.2.2.2         600               131194/131195   LDP     B     257      Blocked
```

Use the **display l2vpn pw** command on NPE 1 to view the PW state.

```
[NPE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 4, 4 up, 0 blocked, 0 down, 0 defect

VSI Name: user_a
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
2.2.2.2         500               131199/131199   LDP     M     256      Up
3.3.3.3         500               131198/131198   LDP     M     257      Up
4.4.4.4         500               131197/131197   LDP     M     258      Up
11.1.1.1        500               131196/131196   LDP     MN    259      Up

VSI Name: user_b
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
2.2.2.2         600               131195/131195   LDP     M     256      Up
3.3.3.3         600               131194/131194   LDP     M     257      Up
4.4.4.4         600               131193/131193   LDP     M     258      Up
11.1.1.1        600               131192/131192   LDP     MN    259      Up
```

Use ping to identify whether hosts within the same VLAN but at different sites can reach each other. If the ping operation succeeds, the VPLS is created successfully.

Configuration files

Only the configuration file for H-VPLS is provided. The configuration for CEs and the routing protocol configuration between PEs are not shown.

- UPE 1

```
#
 mpls lsr-id 11.1.1.1
#
vlan 10 to 11
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  revertive wtr 120
  peer 1.1.1.1 pw-id 500
   backup-peer 2.2.2.2 pw-id 500
#
vsi user_b
 pwsignaling ldp
  revertive wtr 120
  peer 1.1.1.1 pw-id 600
   backup-peer 2.2.2.2 pw-id 600
#
interface LoopBack0
 ip address 11.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 11.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface11
 ip address 11.1.3.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_b
#
```

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_b
#
```

- NPE 1

```
#
 mpls lsr-id 1.1.1.1
#
vlan 10
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 2.2.2.2 pw-id 500
  peer 3.3.3.3 pw-id 500
  peer 4.4.4.4 pw-id 500
  peer 11.1.1.1 pw-id 500 no-split-horizon
#
vsi user_b
 pwsignaling ldp
  peer 2.2.2.2 pw-id 600
  peer 3.3.3.3 pw-id 600
  peer 4.4.4.4 pw-id 600
  peer 11.1.1.1 pw-id 600 no-split-horizon
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Vlan-interface10
 ip address 11.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
```

- NPE 2

```
#
 mpls lsr-id 2.2.2.2
#
vlan 11
#
mpls ldp
```

```
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 500
  peer 3.3.3.3 pw-id 500
  peer 4.4.4.4 pw-id 500
  peer 11.1.1.1 pw-id 500 no-split-horizon
#
vsi user_b
 pwsignaling ldp
  peer 1.1.1.1 pw-id 600
  peer 3.3.3.3 pw-id 600
  peer 4.4.4.4 pw-id 600
  peer 11.1.1.1 pw-id 600 no-split-horizon
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface11
 ip address 11.1.3.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
```

- UPE 2

```
#
 mpls lsr-id 14.1.1.1
#
vlan 12 to 13
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  revertive wtr 120
  peer 3.3.3.3 pw-id 500
   backup-peer 4.4.4.4 pw-id 500
#
vsi user_b
 pwsignaling ldp
  revertive wtr 120
  peer 3.3.3.3 pw-id 600
   backup-peer 4.4.4.4 pw-id 600
#
interface LoopBack0
```

```
 ip address 14.1.1.1 255.255.255.255
#
interface Vlan-interface12
 ip address 20.1.1.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Vlan-interface13
 ip address 20.1.2.1 255.255.255.0
 mpls enable
 mpls ldp enable
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 100
  xconnect vsi user_a
 service-instance 2000
  encapsulation s-vid 200
  xconnect vsi user_b
#
```

- NPE 3

```
#
 mpls lsr-id 3.3.3.3
#
vlan 13
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 500
  peer 2.2.2.2 pw-id 500
  peer 4.4.4.4 pw-id 500
  peer 14.1.1.1 pw-id 500 no-split-horizon
#
vsi user_b
 pwsignaling ldp
  peer 1.1.1.1 pw-id 600
  peer 2.2.2.2 pw-id 600
  peer 4.4.4.4 pw-id 600
  peer 14.1.1.1 pw-id 600 no-split-horizon
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
```

```
interface Vlan-interface13
 ip address 20.1.2.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
```

- NPE 4

```
#
 mpls lsr-id 4.4.4.4
#
vlan 12
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 600
  peer 2.2.2.2 pw-id 600
  peer 3.3.3.3 pw-id 600
  peer 14.1.1.1 pw-id 600 no-split-horizon
#
vsi user_b
 pwsignaling ldp
  peer 1.1.1.1 pw-id 600
  peer 2.2.2.2 pw-id 600
  peer 3.3.3.3 pw-id 600
  peer 14.1.1.1 pw-id 600 no-split-horizon
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface12
 ip address 20.1.1.2 255.255.255.0
 mpls enable
 mpls ldp enable
#
```

Example: Configuring H-VPLS (QinQ access)

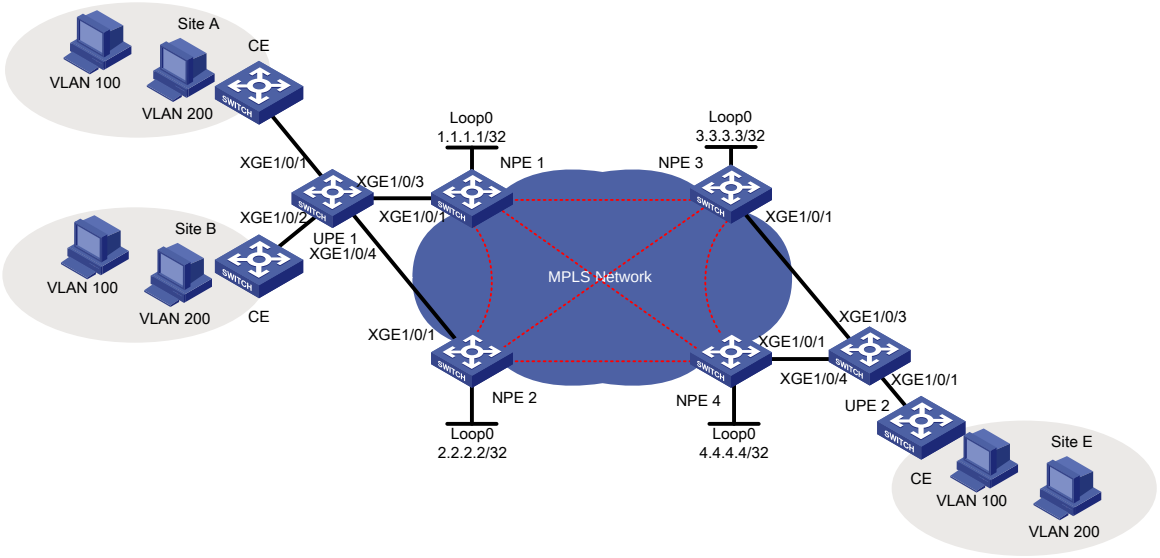
Network configuration

A provider provides VPLS service, with numerous users in various locations. To simplify the network structure and reduce device load and maintenance workload, deploy H-VPLS on the network.

As shown in Figure 5, make sure the following requirements are met:

- Branches at different locations connect to the carrier MPLS network through UPEs that do not support MPLS L2VPN.
- NPEs connect to the UPEs by using the QinQ access mode.
- The UPEs are dual homed to two NPEs for increased reliability.

Figure 5 Network diagram



Analysis

- On the downlink port of each UPE, configure QinQ for NPEs identify user traffic by outer label.
- Use STP to provide loop protection and redundancy for the links.
- On the downlink port of each NPE, configure service instances to match user packets by outer label to transmit user packets over the associated PW.
- To negotiate inner labels, establish remote LDP peer relationships between any two NPEs.

Applicable hardware and software versions

Table 5 Applicable hardware and software versions

Hardware	Software version
S6812 series S6813 series	Release 6628Pxx series
S6550XE-HI series	Release 8106Pxx
S6525XE-HI series	Release 8106Pxx
S5850 series	Unsupported
S5570S-EI series	Unsupported
S5560X-EI series	Release 6628Pxx
S5560X-HI series	Release 6628Pxx
S5500V2-EI series	Release 6628Pxx series

Hardware	Software version
MS4520V2-30F	Release 6628Pxx series
MS4520V2-30C MS4520V2-54C	Release 6628Pxx series
MS4520V2-28S MS4520V2-24TP	Unsupported
S6520X-HI series S6520X-EI series	Release 6628Pxx series
S6520X-SI series S6520-SI series	Release 6628Pxx series
S5000-EI series	Release 6628Pxx series
MS4600 series	Release 6628Pxx series
ES5500 series	Release 6628Pxx series
S5560S-EI series S5560S-SI series	Unsupported
S5500V3-24P-SI S5500V3-48P-SI	Unsupported
S5500V3-SI series (excluding the S5500V3-24P-SI and S5500V3-48P-SI)	Unsupported
S5170-EI series	Unsupported
S5130S-HI series S5130S-EI series S5130S-SI series S5130S-LI series	Unsupported
S5120V2-SI series S5120V2-LI Series	Unsupported
S5120V3-EI series	Unsupported
S5120V3-36F-SI S5120V3-28P-HPWR-SI S5120V3-54P-PWR-SI	Unsupported
S5120V3-SI series (excluding S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Unsupported
S5120V3-LI series	Unsupported
S3600V3-EI series	Unsupported
S3600V3-SI series	Unsupported
S3100V3-EI series S3100V3-SI series	Unsupported
S5110V2 series	Unsupported
S5110V2-SI series	Unsupported

Hardware	Software version
S5000V3-EI series S5000V5-EI series	Unsupported
S5000E-X series S5000X-EI series	Unsupported
E128C E152C E500C series E500D series	Unsupported
MS4320V2 series MS4320V3 series MS4300V2 series MS4320 series MS4200 series	Unsupported
WS5850-WiNet series	Unsupported
WS5820-WiNet series WS5810-WiNet series	Unsupported
WAS6000 series	Unsupported
IE4300-12P-AC & IE4300-12P-PWR IE4300-M series IE4320 series	Unsupported
S5135S-EI series	Unsupported

Procedure

Configuring basic network settings

1. Configure IGP on the MPLS backbone network to ensure that all interfaces on NPEs are reachable to each other. (Details not shown.)
2. Configure basic MPLS and MPLS LDP on the backbone network to establish LDP LSPs. (Details not shown.)
3. Configure interfaces on each CE that connect to UPEs as a trunk port and permit packets from VLAN 100 and VLAN 200 to pass through with tags. (Details not shown.)

Configuring UPE 1

Configure UPE1 to operate in PVST mode to avoid loops.

```
<UPE1> system-view
[UPE1] stp global enable
[UPE1] stp mode pvst
```

Assign Ten-GigabitEthernet 1/0/1to access VLAN 1000 and enable QinQ on the interface.

```
[UPE1] vlan 1000
[UPE1-vlan1000] quit
[UPE1] interface ten-gigabitethernet 1/0/1
[UPE1-Ten-GigabitEthernet1/0/1] port access vlan 1000
[UPE1-Ten-GigabitEthernet1/0/1] qinq enable
[UPE1-Ten-GigabitEthernet1/0/1] quit
```

Assign Ten-GigabitEthernet 1/0/2 to access VLAN 1000 and enable QinQ on the interface.

```
[UPE1] interface ten-gigabitethernet 1/0/2
[UPE1-Ten-GigabitEthernet1/0/2] port access vlan 1000
[UPE1-Ten-GigabitEthernet1/0/2] qinq enable
[UPE1-Ten-GigabitEthernet1/0/2] quit
```

Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and permit tagged packets from VLAN 1000 to be transmitted to NPE 1.

```
[UPE1] interface ten-gigabitethernet 1/0/3
[UPE1-Ten-GigabitEthernet1/0/3] port link-type trunk
[UPE1-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1000
[UPE1-Ten-GigabitEthernet1/0/3] quit
```

Configure Ten-GigabitEthernet 1/0/4 as a trunk port, and permit tagged packets from VLAN 1000 to be transmitted to NPE 2.

```
[UPE1] interface ten-gigabitethernet 1/0/4
[UPE1-Ten-GigabitEthernet1/0/4] port link-type trunk
[UPE1-Ten-GigabitEthernet1/0/4] port trunk permit vlan 1000
[UPE1-Ten-GigabitEthernet1/0/4] quit
```

Configuring NPE 1

Enable MPLS L2VPN.

```
[NPE1] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[NPE1] vsi user_a
[NPE1-vsi-user_a] pwsignaling ldp
```

Specify NPE 2, NPE 3, and NPE 4 as the remote peers.

```
[NPE1-vsi-user_a-ldp] peer 2.2.2.2 pw-id 500
[NPE1-vsi-user_a-ldp-2.2.2.2-500] quit
[NPE1-vsi-user_a-ldp] peer 3.3.3.3 pw-id 500
[NPE1-vsi-user_a-ldp-3.3.3.3-500] quit
[NPE1-vsi-user_a-ldp] peer 4.4.4.4 pw-id 500
[NPE1-vsi-user_a-ldp-4.4.4.4-500] quit
[NPE1-vsi-user_a-ldp] quit
[NPE1-vsi-user_a] quit
```

Create service instance 1000 on Ten-GigabitEthernet 1/0/1 that connects to UPE 1 to match packets from VLAN 1000 and bind the service instance to VSI **user_a**. Because upstream packets carry the service provider VLAN, the AC access mode must be VLAN (optional, defaulting to VLAN mode).

```
[NPE1] interface ten-gigabitethernet 1/0/1
[NPE1-Ten-GigabitEthernet1/0/1] service-instance 1000
[NPE1-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 1000
[NPE1-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi user_a access-mode vlan
[NPE1-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Configuring NPE 2

The configuration for NPE 2 is similar to that for NPE 1 except that the NPE peers for them are different. For more information about the configuration, see the configuration file.

Configuring UPE 2

Configure UPE2 to operate in PVST mode to avoid loops.

```
<UPE2> system-view
```

```
[UPE2] stp global enable
[UPE2] stp mode pvst
```

Assign Ten-GigabitEthernet 1/0/1to access VLAN 1000 and enable QinQ on the interface.

```
[UPE2] vlan 1000
[UPE2-vlan1000] quit
[UPE2] interface ten-gigabitethernet 1/0/1
[UPE2-Ten-GigabitEthernet1/0/1] port access vlan 1000
[UPE2-Ten-GigabitEthernet1/0/1] qinq enable
[UPE2-Ten-GigabitEthernet1/0/1] quit
```

Configure Ten-GigabitEthernet 1/0/3 as a trunk port, and permit tagged packets from VLAN 1000 to be transmitted to NPE 3.

```
[UPE2] interface ten-gigabitethernet 1/0/3
[UPE2-Ten-GigabitEthernet1/0/3] port link-type trunk
[UPE2-Ten-GigabitEthernet1/0/3] port trunk permit vlan 1000
[UPE2-Ten-GigabitEthernet1/0/3] quit
```

Configure Ten-GigabitEthernet 1/0/4 as a trunk port, and permit tagged packets from VLAN 1000 to be transmitted to NPE 4.

```
[UPE2] interface ten-gigabitethernet 1/0/4
[UPE2-Ten-GigabitEthernet1/0/4] port link-type trunk
[UPE2-Ten-GigabitEthernet1/0/4] port trunk permit vlan 1000
[UPE2-Ten-GigabitEthernet1/0/4] quit
```

Configuring NPE 3

Enable MPLS L2VPN.

```
[NPE3] l2vpn enable
```

Configure VSI **user_a** that uses LDP as the PW signaling protocol.

```
[NPE3] vsi user_a
[NPE3-vsi-user_a] pwsignaling ldp
```

Specify NPE 1, NPE 2, and NPE 4 as the peer NPEs.

```
[NPE3-vsi-user_a-ldp] peer 1.1.1.1 pw-id 500
[NPE3-vsi-user_a-ldp-1.1.1.1-500] quit
[NPE3-vsi-user_a-ldp] peer 2.2.2.2 pw-id 500
[NPE3-vsi-user_a-ldp-2.2.2.2-500] quit
[NPE3-vsi-user_a-ldp] peer 4.4.4.4 pw-id 500
[NPE3-vsi-user_a-ldp-4.4.4.4-500] quit
[NPE3-vsi-user_a-ldp] quit
[NPE3-vsi-user_a] quit
```

Create service instance 1000 on Ten-GigabitEthernet 1/0/1 of UPE 2 to match packets from VLAN 1000 and bind the service instance to VSI **user_a**. Because upstream packets carry the carrier's VLAN, the AC access mode must be VLAN (optional, defaulting to VLAN mode).

```
[NPE3] interface ten-gigabitethernet 1/0/1
[NPE3-Ten-GigabitEthernet1/0/1] service-instance 1000
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 1000
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] xconnect vsi user_a access-mode vlan
[NPE3-Ten-GigabitEthernet1/0/1-srv1000] quit
```

Configuring NPE 4

The configuration for NPE 4 is similar to that for NPE 3 except that the NPE peers for them are different. For more information about the configuration, see the configuration file.

Verifying the configuration

Verify the state of PWs on each NPE. The following uses NPE 1 as an example.

Use the **display l2vpn pw** command on NPE 1 to view the PW state.

```
[NPE1] display l2vpn pw
Flags: M - main, B - backup, H - hub link, S - spoke link, N - no split horizon
Total number of PWs: 3, 3 up, 0 blocked, 0 down, 0 defect

VSI Name: user_a
Peer            PW ID/Rmt Site    In/Out Label    Proto   Flag  Link ID  State
2.2.2.2         500               131199/131199   LDP     M     256      Up
3.3.3.3         500               131198/131198   LDP     M     257      Up
4.4.4.4         500               131197/131197   LDP     M     258      Up
```

Use ping to identify whether hosts within the same VLAN but at different sites can reach each other. If the ping operation succeeds, the VPLS is created successfully.

Configuration files

Only the configuration file for H-VPLS is provided. The configuration for CEs and the routing protocol configuration between PEs are not shown.

- UPE 1

```
#
vlan 1000
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 1000
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 1000
#
```

- NPE 1

```
#
 mpls lsr-id 1.1.1.1
```

```
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 2.2.2.2 pw-id 500
  peer 3.3.3.3 pw-id 500
  peer 4.4.4.4 pw-id 500
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
#
```

- NPE 2

```
#
 mpls lsr-id 2.2.2.2
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 500
  peer 3.3.3.3 pw-id 500
  peer 4.4.4.4 pw-id 500
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
#
```

- UPE 2

```
#
vlan 1000
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 1000
 qinq enable
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan 1 1000
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 1000
#
```

- NPE 3

```
#
 mpls lsr-id 3.3.3.3
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 500
  peer 2.2.2.2 pw-id 500
  peer 4.4.4.4 pw-id 500
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
#
```

- NPE 4

```
#
 mpls lsr-id 4.4.4.4
#
mpls ldp
#
 l2vpn enable
#
vsi user_a
 pwsignaling ldp
  peer 1.1.1.1 pw-id 500
  peer 2.2.2.2 pw-id 500
  peer 3.3.3.3 pw-id 500
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 service-instance 1000
  encapsulation s-vid 1000
  xconnect vsi user_a
#
```

Contents

Introduction

This document provides SR-MPLS configuration examples.

Segment Routing (SR) is a source routing technology. The source node selects a path for the packets, and then encodes the path in the packet header as an ordered list of segments. Each segment is identified by the segment identifier (SID). The SR nodes along the path forward the packets based on the SIDs in the packets. Only the source node needs to maintain the path status. SR can operate with MPLS. In an MPLS network, SR uses MPLS labels as SIDs to forward packets on an LSP.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

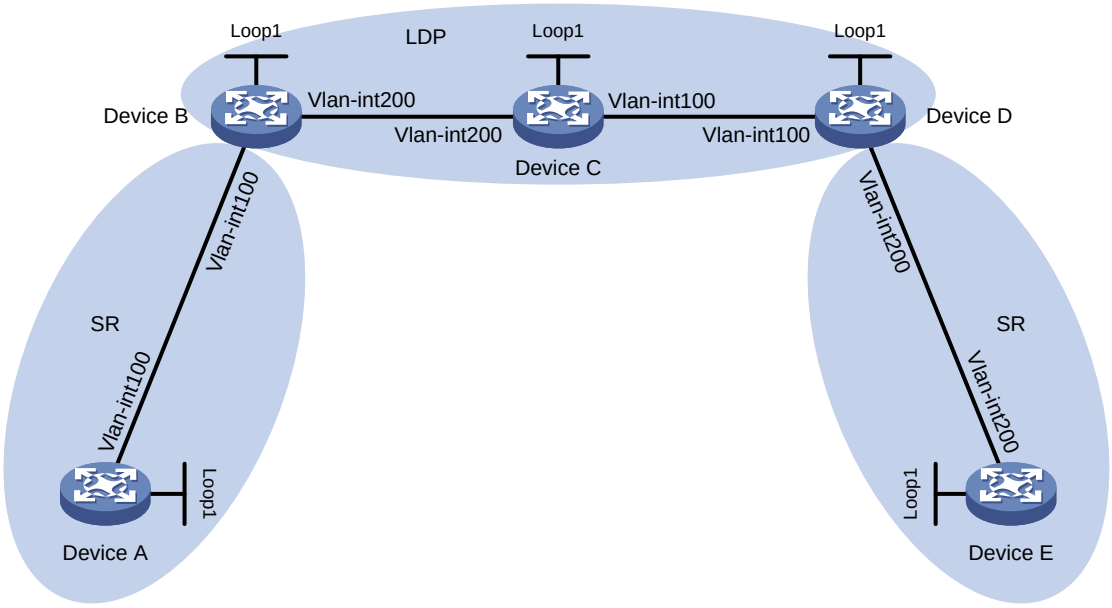
The following information is provided based on the assumption that you have basic knowledge of SR-MPLS.

Example: Configuring SR-MPLS over LDP for network connections

Network configuration

As shown in Figure 1, the SR-MPLS network is segmented by an LDP network. To enable communication between the two SR-MPLS network segments across the LDP network, establish label connectivity between the SR-MPLS and LDP networks. When Device A forwards traffic to Device E through the related SRLSP, you must configure both Device B and Device D to ensure that the two SR-MPLS network segments can communicate across the LDP network.

Figure 1 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Device A	Loop1	1.1.1.1/32	Device B	Loop1	2.2.2.2/32
	Vlan-Int100	10.0.0.1/24		Vlan-Int100	10.0.0.2/24
Device C	Loop1	3.3.3.3/32		Vlan-Int200	11.0.0.1/24
	Vlan-Int100	12.0.0.1/24	Device D	Loop1	4.4.4.4/32
	Vlan-Int200	11.0.0.2/24		Vlan-Int100	12.0.0.2/24
Device E	Loop1	5.5.5.5/32		Vlan-Int200	13.0.0.1/24
	Vlan-Int200	13.0.0.2/24			

Analysis

- Configure Device A, Device B, Device C, Device D, and Device E to run IS-IS.
- Configure Device B, Device C, and Device D to run LDP.
- Configure Device A, Device B, Device D, and Device E to run SR-MPLS.

Applicable hardware and software versions

Product	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported

S5570S-EI switch series	Not supported
S5560X-EI switch series	Not supported
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Not supported
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported

S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Procedures

Configuring Device A

Configure IP addresses and masks for interfaces. (Details not shown.)

Configure IS-IS to achieve network level connectivity and set the IS-IS cost style to **wide**.

```
<DeviceA> system-view
[DeviceA] isis 1
[DeviceA-isis-1] network-entity 00.0000.0000.0001.00
[DeviceA-isis-1] cost-style wide
[DeviceA-isis-1] quit
[DeviceA] interface vlan-interface 100
[DeviceA-Vlan-interface100] isis enable 1
[DeviceA-Vlan-interface100] quit
[DeviceA] interface loopback 1
[DeviceA-LoopBack1] isis enable 1
[DeviceA-LoopBack1] quit
```

Configure an MPLS LSR ID.

```
[DeviceA] mpls lsr-id 1.1.1.1
```

Enable SR-MPLS for IS-IS.

```
[DeviceA] isis 1
[DeviceA-isis-1] address-family ipv4
[DeviceA-isis-1-ipv4] segment-routing mpls
[DeviceA-isis-1-ipv4] quit
```

Configure an MPLS SRGB.

```
[DeviceA-isis-1] segment-routing global-block 16000 16999
[DeviceA-isis-1] quit
```

Configure an IS-IS prefix SID.

```
[DeviceA] interface loopback 1
[DeviceA-LoopBack1] isis prefix-sid index 10
[DeviceA-LoopBack1] quit
```

Configuring Device B

Configure IP addresses and masks for interfaces. (Details not shown.)

Configure IS-IS to achieve network level connectivity and set the IS-IS cost style to **wide**.

```
<DeviceB> system-view
[DeviceB] isis 1
[DeviceB-isis-1] network-entity 00.0000.0000.0002.00
[DeviceB-isis-1] cost-style wide
[DeviceB-isis-1] quit
[DeviceB] interface vlan-interface 100
[DeviceB-Vlan-interface100] isis enable 1
[DeviceB-Vlan-interface100] quit
[DeviceB] interface vlan-interface 200
[DeviceB-Vlan-interface200] isis enable 1
[DeviceB-Vlan-interface200] quit
[DeviceB] interface loopback 1
[DeviceB-LoopBack1] isis enable 1
[DeviceB-LoopBack1] quit
```

Configure an MPLS LSR ID.

```
[DeviceB] mpls lsr-id 2.2.2.2
```

Configure LDP.

```
[DeviceB] mpls ldp
[DeviceB-ldp] quit
[DeviceB] interface vlan-interface 200
[DeviceB-Vlan-interface200] mpls enable
[DeviceB-Vlan-interface200] mpls ldp enable
[DeviceB-Vlan-interface200] quit
```

Enable SR-MPLS for IS-IS.

```
[DeviceB] isis 1
[DeviceB-isis-1] address-family ipv4
[DeviceB-isis-1-ipv4] segment-routing mpls
[DeviceB-isis-1-ipv4] quit
```

Configure an MPLS SRGB.

```
[DeviceB-isis-1] segment-routing global-block 17000 17999
[DeviceB-isis-1] quit
```

Configure an IS-IS prefix SID.

```
[DeviceB] interface loopback 1
[DeviceB-LoopBack1] isis prefix-sid index 20
[DeviceB-LoopBack1] quit
```

Configuring Device C

Configure IP addresses and masks for interfaces. (Details not shown.)

Configure IS-IS to achieve network level connectivity and set the IS-IS cost style to **wide**.

```
<DeviceC> system-view
[DeviceC] isis 1
[DeviceC-isis-1] network-entity 00.0000.0000.0003.00
[DeviceC-isis-1] cost-style wide
[DeviceC-isis-1] quit
[DeviceC] interface vlan-interface 100
[DeviceC-Vlan-interface100] isis enable 1
[DeviceC-Vlan-interface100] quit
[DeviceC] interface vlan-interface 200
[DeviceC-Vlan-interface200] isis enable 1
[DeviceC-Vlan-interface200] quit
[DeviceC] interface loopback 1
[DeviceC-LoopBack1] isis enable 1
[DeviceC-LoopBack1] quit
```

Configure an MPLS LSR ID.

```
[DeviceC] mpls lsr-id 3.3.3.3
```

Configure LDP.

```
[DeviceC] mpls ldp
[DeviceC-ldp] quit
[DeviceC] interface vlan-interface 100
[DeviceC-Vlan-interface100] mpls enable
[DeviceC-Vlan-interface100] mpls ldp enable
[DeviceC-Vlan-interface100] quit
[DeviceC] interface vlan-interface 200
[DeviceC-Vlan-interface200] mpls enable
[DeviceC-Vlan-interface200] mpls ldp enable
[DeviceC-Vlan-interface200] quit
```

Configuring Device D

Configure IP addresses and masks for interfaces. (Details not shown.)

Configure IS-IS to achieve network level connectivity and set the IS-IS cost style to **wide**.

```
<DeviceD> system-view
[DeviceD] isis 1
[DeviceD-isis-1] network-entity 00.0000.0000.0004.00
[DeviceD-isis-1] cost-style wide
[DeviceD-isis-1] quit
[DeviceD] interface vlan-interface 100
[DeviceD-Vlan-interface100] isis enable 1
[DeviceD-Vlan-interface100] quit
[DeviceD] interface vlan-interface 200
[DeviceD-Vlan-interface200] isis enable 1
[DeviceD-Vlan-interface200] quit
[DeviceD] interface loopback 1
[DeviceD-LoopBack1] isis enable 1
[DeviceD-LoopBack1] quit
```

Configure an MPLS LSR ID.

```
[DeviceD] mpls lsr-id 4.4.4.4
```

Configure LDP.

```
[DeviceD] mpls ldp
[DeviceD-ldp] quit
[DeviceD] interface vlan-interface 100
[DeviceD-Vlan-interface1001] mpls enable
[DeviceD-Vlan-interface100] mpls ldp enable
[DeviceD-Vlan-interface100] quit
```

Enable SR-MPLS for IS-IS.

```
[DeviceD] isis 1
[DeviceD-isis-1] address-family ipv4
[DeviceD-isis-1-ipv4] segment-routing mpls
[DeviceD-isis-1-ipv4] quit
```

Configure an MPLS SRGB.

```
[DeviceD-isis-1] segment-routing global-block 18000 18999
[DeviceD-isis-1] quit
```

Configure an IS-IS prefix SID.

```
[DeviceD] interface loopback 1
[DeviceD-LoopBack1] isis prefix-sid index 40
[DeviceD-LoopBack1] quit
```

Configuring Device E

Configure IP addresses and masks for interfaces. (Details not shown.)

Configure IS-IS to achieve network level connectivity and set the IS-IS cost style to **wide**.

```
<DeviceE> system-view
[DeviceE] isis 1
[DeviceE-isis-1] network-entity 00.0000.0000.0005.00
[DeviceE-isis-1] cost-style wide
[DeviceE-isis-1] quit
[DeviceE] interface vlan-interface 200
[DeviceE-Vlan-interface200] isis enable 1
[DeviceE-Vlan-interface200] quit
[DeviceE] interface loopback 1
[DeviceE-LoopBack1] isis enable 1
[DeviceE-LoopBack1] quit
```

Configure an MPLS LSR ID.

```
[DeviceE] mpls lsr-id 5.5.5.5
```

Enable SR-MPLS for IS-IS.

```
[DeviceE] isis 1
[DeviceE-isis-1] address-family ipv4
[DeviceE-isis-1-ipv4] segment-routing mpls
[DeviceE-isis-1-ipv4] quit
```

Configure an MPLS SRGB.

```
[DeviceE-isis-1] segment-routing global-block 19000 19999
[DeviceE-isis-1] quit
```

Configure an IS-IS prefix SID.

```
[DeviceE] interface loopback 1
[DeviceE-LoopBack1] isis prefix-sid index 50
[DeviceE-LoopBack1] quit
```

Verifying the configuration

Display LDP LSP information on Device B.

```
[DeviceB] display mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup, N/A - unavailable
FECs: 5           Ingress: 3           Transit: 3           Egress: 2

FEC                In/Out Label        Nexthop         OutInterface
1.1.1.1/32         24116/-
                   -/24117(L)
2.2.2.2/32         3/-
                   -/24120(L)
3.3.3.3/32         -/3                 11.0.0.2        Vlan200
                   24121/3             11.0.0.2        Vlan200
4.4.4.4/32         -/24119             11.0.0.2        Vlan200
                   24118/24119         11.0.0.2        Vlan200
5.5.5.5/32         -/24118             11.0.0.2        Vlan200
                   24117/24118         11.0.0.2        Vlan200
```

Display IS-IS SRLSP information on Device B.

```
[DeviceB] display mpls lsp protocol isis
FEC                         Proto       In/Out Label    Interface/Out NHLFE
1.1.1.1/32                  ISIS        17010/3         Vlan100
1.1.1.1/32                  ISIS        -/3             Vlan100
2.2.2.2/32                  ISIS        17020/-         -
4.4.4.4/32                  ISIS        17040/24119     Vlan200
4.4.4.4/32                  ISIS        -/24119         Vlan200
5.5.5.5/32                  ISIS        17050/24118     Vlan200
5.5.5.5/32                  ISIS        -/24118         Vlan200
```

The output shows that the IS-IS SRLSP entries for Device D and Device E are using LDP outgoing labels.

Configuration files

Device A

```
#
isis 1
 cost-style wide
 segment-routing global-block 16000 16999
 network-entity 00.0000.0000.0001.00
 #
 address-family ipv4 unicast
  segment-routing mpls
#
 mpls lsr-id 1.1.1.1
#
vlan 1
#
vlan 100
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
 isis prefix-sid index 10
#
interface Vlan-interface100
 ip address 10.0.0.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 combo enable fiber
#
```

Device B

```
#
isis 1
 cost-style wide
 segment-routing global-block 17000 17999
 network-entity 00.0000.0000.0002.00
 #
 address-family ipv4 unicast
  segment-routing mpls
#
 mpls lsr-id 2.2.2.2
#
vlan 1
#
vlan 100
#
vlan 200
#
mpls ldp
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
 isis prefix-sid index 20
#
interface Vlan-interface100
 ip address 10.0.0.2 255.255.255.0
 isis enable 1
#
interface Vlan-interface200
 ip address 11.0.0.1 255.255.255.0
 isis enable 1
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 combo enable fiber
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
 combo enable fiber
#
```

Device C

```
#
isis 1
 cost-style wide
 network-entity 00.0000.0000.0003.00
#
 mpls lsr-id 3.3.3.3
#
vlan 1
#
vlan 100
#
vlan 200
#
mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
interface Vlan-interface100
 ip address 12.0.0.1 255.255.255.0
 isis enable 1
 mpls enable
 mpls ldp enable
#
interface Vlan-interface200
 ip address 11.0.0.2 255.255.255.0
 isis enable 1
 mpls enable
 mpls ldp enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
 combo enable fiber
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 100
 combo enable fiber
#
```

Device D

```
#
isis 1
 cost-style wide
 segment-routing global-block 18000 18999
 network-entity 00.0000.0000.0004.00
 #
 address-family ipv4 unicast
  segment-routing mpls
#
 mpls lsr-id 4.4.4.4
#
vlan 1
#
vlan 100
#
vlan 200
#
mpls ldp
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
 isis prefix-sid index 40
#
interface Vlan-interface100
 ip address 12.0.0.2 255.255.255.0
 isis enable 1
 mpls enable
 mpls ldp enable
#
interface Vlan-interface200
 ip address 13.0.0.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
 combo enable fiber
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
 combo enable fiber
#
```

Device E

```
#
isis 1
 cost-style wide
 segment-routing global-block 19000 19999
 network-entity 00.0000.0000.0005.00
 #
 address-family ipv4 unicast
  segment-routing mpls
#
 mpls lsr-id 5.5.5.5
#
vlan 1
#
vlan 200
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
 isis prefix-sid index 50
#
interface Vlan-interface200
 ip address 13.0.0.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
 combo enable fiber
#
```

Contents

Introduction

The following information provides automated VCF fabric deployment configuration examples.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of automated VCF fabric deployment.

Example: Configuring automated deployment for the distributed gateway

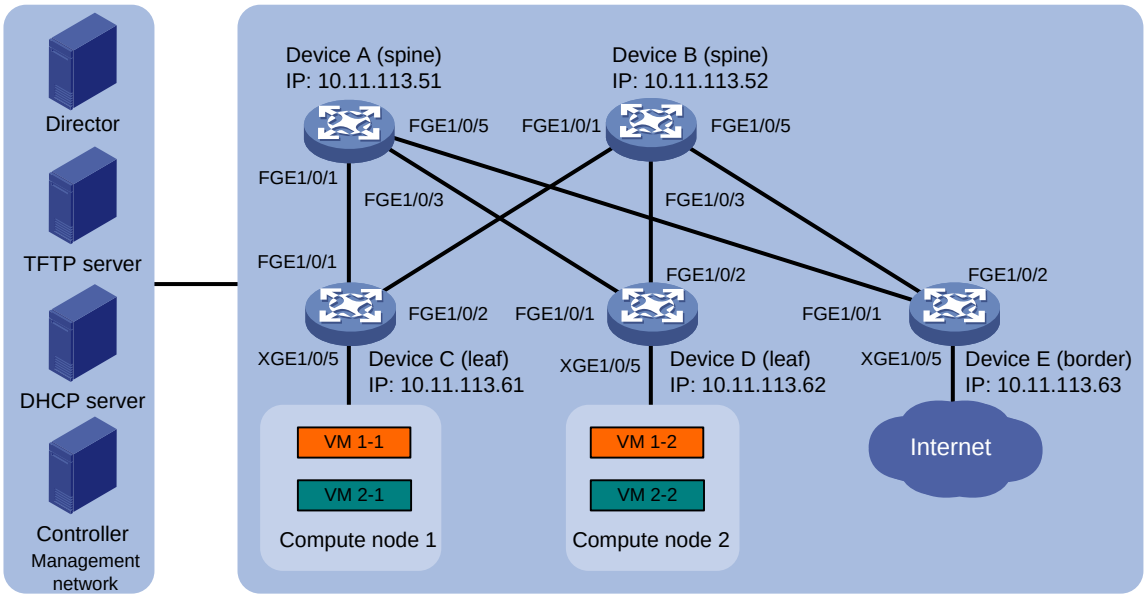
Network configuration

As shown in Figure 1, the distributed VXLAN IP gateway network adopts a spine/leaf architecture. Device A and Device B are spine nodes. Device C and Device D are leaf nodes, which form the distributed VXLAN IP gateway. Device E is a border device and also serves as the border gateway connected to the WAN. Device A to Device E connect to the Director server, DHCP server, and NTP server in the management network through management Ethernet interfaces.

Configure automated VCF fabric deployment to meet the following requirements:

- The DHCP server dynamically allocates IP addresses from the 10.11.113.0/24 network segment to devices.
- After the initial power-on of Device A to Device E, they can automatically complete the automated underlay network deployment based on the template file issued by the Director server.
- Create VM 1-1 and VM 1-2 for tenant **a** on compute node 1 and compute node 2 respectively. Create VM 2-1 and VM 2-2 for tenant 2. Implement Layer 2 communication within the same VXLAN, and implement communication between different VXLANs and between a VXLAN and WAN through the distributed VXLAN gateway.

Figure 1 Network diagram



Analysis

- Connect the devices and connect the devices and servers to make sure the devices in the network can communicate with one another.
- Configure the DHCP, TFTP, and NTP servers to make sure they can operate correctly.
- This example uses the H3C DR2000 as the Director server for the automated underlay network deployment. The deployment process is visualized, and the devices are automatically incorporated when the deployment is completed. For more information about DR2000 servers, see the user guide of the product. The procedure described in "Configuring the Director server" is for illustration only.
- Perform automated overlay network deployment to ensure configuration consistency on the devices. This document takes the open-source OpenStack Controller system as an example to briefly introduce the deployment process. For more information about the deployment if you choose the solution that uses CloudOS with the VCFC controller, see the H3C VCF fabric solution guide or official documentation based on the installed software version.

Restrictions and guidelines

- The distributed gateway requires configuring the same MAC address for the same VSI interface on each leaf node. This ensures gateway consistency upon VM migrations.
- The spine node for the distributed gateway is only used as the core forwarding point in the underlay network. No overlay network configuration is required.

Applicable hardware and software versions

Table 1 Applicable hardware and software versions

Product	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Not supported
MS4520V2-30F switch	Not supported
MS4520V2-30C switch MS4520V2-54C switch	Not supported
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Release 63xx (not supported by the S5560S-SI switch series)
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI series	Release 63xx (not supported by the S5130S-SI and S5130S-LI switch series)
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Product	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Release 63xx (not supported by the S3100V3-SI switch series)
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Release 63xx
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 series MS4200 series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Release 66xx
S5135S-EI switch series	Not supported

Configuring automated deployment

Configuring the DHCP server

Configure the following DHCP server settings:

- DHCP address pool: Specify network segment 10.11.113.0/24 for dynamic address allocation.
- TFTP server IP address: 10.11.113.19/24.
- Startup file name: **aaa.template**.

The file name obtained by the device might vary by device role, such as **aaa_leaf.template** or **aaa_spine.template**.

Configuring the Director server

1. Install Director and complete the installation of components such as UBA and network traffic analysis (NTA).
2. Install the DHCP plug to enable AD-DC to set a fixed IP address for the server.
3. Complete basic automated deployment settings, such as network topology type, network scale, and network segments that can be provided by DHCP.
4. Set up network automation parameters, including the MAC address of the master spine node in the network topology, the assignable underlay IP address segment for the master spine node, username, password, user role, and Neutron server parameters.

Deploying the controller node

Deploy the controller node for open-source OpenStack as follows (the procedure is for illustration only):

1. Install the MySQL database.
2. Install RabbitMQ.
3. Install and verify the following services, including adding OpenStack Identity service, creating OpenStack client, and adding image service, nova service, and neutron service.

Deploying compute nodes

Deploy compute nodes for open-source OpenStack as follows (the procedure is for illustration only):

1. Install OpenStack Nova compute components, openvswitch, and neutron ovs agent.

2. Configure management component parameters, including IP address, username, and username and password for communication with RabbitMQ.
3. Restart compute node services.
4. After completing compute node deployment, install Dashboard on the controller node and verify the compute node installation result. You can see the records for the newly added compute nodes, compute node1 and compute node2.

Starting the automated deployment process

Automated underlay network deployment

After the network setup and server configuration are completed, each device (Device A through Device E) starts up without loading configuration to complete the automated underlay network deployment as follows:

1. Obtains an IP address, the IP address of the TFTP server, and a template file name from the DHCP server.
2. Downloads the template file based on the device role from the TFTP server.
3. Parses the template file and compares the current software version with the software version in the template file. If the two versions are inconsistent, the device downloads the new software version.
4. Parses the template file and deploys static configurations.
5. The master spine node Device A uses NETCONF to issue configurations such as loopback IP to Devices B through Device E.
6. Configure IP settings for the interconnect interfaces between spine and leaf nodes, and start the routing protocol to implement Layer 3 VTEP IP connectivity.

NOTE:

After completing the underlay automation, execute the **save** command on the master spine device to save the configurations such as address allocation. This prevents repeated address allocation for the devices upon restart of the master spine device.

Deploying tenant overlay network and completing automated device deployment

1. Create a network named **Network** on the Dashboard.
2. Create two subnets named **subnet-1** and **subnet-2** on the Dashboard and configure their network addresses.
3. Create a router named **router** on the Dashboard, and bind the router's interfaces with the two subnets.
4. Create VM 1-1 and VM 1-2 on compute node 1, and create VM 2-1 and VM 2-2 on compute node 2.

Verifying the configuration

1. Verify underlay topology information:

Display VCF fabric topology information on spine node Device A.

```
[DeviceA] display vcf-fabric topology
                                  Topology Information
------------------------------------------------------------------------------
-
* indicates the master spine role among all spines
SpineIP           Interface                     Link LeafIP           Status
*10.11.113.51     FortyGigE1/0/1                Up   10.11.113.61     Deploying
                  FortyGigE1/0/2                Down --
 --
                  FortyGigE1/0/3                Up   10.11.113.62
Deploying
                  FortyGigE1/0/4                Down --                       --
                  FortyGigE1/0/5                Up   10.11.113.63     Deploying
                  FortyGigE1/0/6                Down --                       --
10.11.113.52      FortyGigE1/0/1                Up   10.11.113.61     Deploying
                  FortyGigE1/0/2                Down --
 --
                  FortyGigE1/0/3                Up   10.11.113.62
Deploying
                  FortyGigE1/0/4                Down --                       --
                  FortyGigE1/0/5                Up   10.11.113.63     Deploying
                  FortyGiE1/0/6                Down --                       --
```

2. Verify automated underlay network deployment:

Display information about automated underlay network deployment on leaf node Device C of the distributed gateway.

```
[DeviceC] display vcf-fabric underlay autoconfigure
success command:
   #
           system
           clock timezone beijing add 08:00:00
         #
           system
           lldp global enable
           lldp compliance cdp
         #
           system
           ospf 1
           non-stop-routing
           area 0.0.0.0
         #
           system
           interface LoopBack0
```

```
#
  system
  l2vpn enable
#
  system
  vxlan tunnel mac-learning disable
  vxlan tunnel arp-learning disable
#
  system
  stp global enable
#
  system
  ntp-service enable
  ntp-service unicast-server 10.11.113.136 vpn-instance mgmt
#
  system
  netconf soap https enable
  netconf ssh server enable
  restful https enable
#
  system
  info-center loghost vpn-instance mgmt 10.11.113.136
#
  system
  local-user admin
  password ******
  service-type https
  authorization-attribute user-role network-admin
#
  system
  line vty 0 63
  authentication-mode scheme
  user-role network-admin
#
  system
  vcf-fabric topology enable
#
  system
  neutron
  rabbit user openstack
  rabbit password ******
  rabbit host ip 10.11.113.136 vpn-instance mgmt
  restful user admin password ******
  vpn-target 1:1 export-extcommunity
  vsi-mac 789c-2f5f-0200
  network-type distributed-vxlan
  l2agent enable
  l3agent enable
```

```
          #
            system
            snmp-agent
            snmp-agent community read public
            snmp-agent community write private
            snmp-agent sys-info version all
            snmp-agent packet max-size 4096
            snmp-agent target-host trap address udp-domain 192.181.1.30 vpn-insta
nce mgmt params securityname public v2c
          #
            system
            telnet server enable
            local-user admin
            password ******
            service-type telnet http https
            authorization-attribute user-role network-admin
          #
            system
            netconf soap http enable
            netconf soap https enable
            local-user admin
            password ******
            service-type http https
            authorization-attribute user-role network-admin
          #
            system
            bgp 100
            non-stop-routing
            address-family l2vpn evpn
          #
Uplink interface:
          FortyGigE1/0/1
          FortyGigE1/0/2
IRF allocation:
          Self Bridge Mac: 00e0-fc00-5100
          IRF Status: No
          Member List: [1]
BGP peer configuration:
          10.100.16.17
          10.100.16.16
```

3. Verify automated overlay network deployment:

Display VSI and VPN instance configurations on leaf node Device C of the distributed gateway.

```
[DeviceC] display current-configuration configuration vsi
#
vsi vxlan10071
 gateway vsi-interface 8190
```

```
 vxlan 10071
 evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
#
return
[DeviceC] display current-configuration interface Vsi-interface
  interface Vsi-interface4091
  ip binding vpn-instance neutron-1015
  ip address 108.1.0.1 255.255.0.0 sub
  mac-address 789c-2f5f-0200
  arp mode uni
  distributed-gateway local
#
[DeviceC] display ip vpn-instance
  Total VPN-Instances configured : 6
  VPN-Instance Name               RD                      Create time
  mgmt                                                    2018/04/17 08:49:59
  neutron-1016                    4227879168:1016         2018/04/17 08:50:59
  neutron-1015                    4227879168:1015         2018/04/17 08:51:01
  neutron-1018                    4227879168:1018         2018/04/17 08:51:03
  neutron-1017                    4227879168:1017         2018/04/17 08:51:07
  neutron-1021                    4227879168:1021         2018/04/17 08:51:08
```

4. Verify connectivity between VMs:

Access the console of VM 1-1 on compute node 1 and execute a ping operation. VM 2-2 on compute node 2 can be pinged successfully.

```
$ ping 10.1.1.3
Ping 10.1.1.3 (10.1.1.3): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.3: icmp_seq=0 ttl=254 time=10.000 ms
56 bytes from 10.1.1.3: icmp_seq=1 ttl=254 time=4.000 ms
56 bytes from 10.1.1.3: icmp_seq=2 ttl=254 time=4.000 ms
56 bytes from 10.1.1.3: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 10.1.1.3: icmp_seq=4 ttl=254 time=3.000 ms
--- Ping statistics for 10.1.1.3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 3.000/4.800/10.000/2.638 ms
```

Configuration files

- Main underlay configuration on leaf node Device C:

```
#
irf mac-address persistent always
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
```

```
#
 vxlan tunnel mac-learning disable
#
ospf 1
 non-stop-routing
 area 0.0.0.0
#
 lldp compliance cdp
 lldp global enable
#
interface LoopBack0
 ip address 19.1.1.254 255.255.255.255
#
interface FortyGigE1/0/1
 port link-mode route
 ip address unnumbered interface LoopBack0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
 lldp compliance admin-status cdp txrx
 lldp management-address arp-learning
 lldp tlv-enable basic-tlv management-address-tlv interface LoopBack0
#
interface FortyGigE1/0/2
 port link-mode route
 ip address unnumbered interface LoopBack0
 ospf network-type p2p
 ospf 1 area 0.0.0.0
 lldp compliance admin-status cdp txrx
 lldp management-address arp-learning
 lldp tlv-enable basic-tlv management-address-tlv interface LoopBack0
#
bgp 100
 non-stop-routing
 peer 200.1.15.152 as-number 100
 peer 200.1.15.152 connect-interface LoopBack0
 peer 200.1.15.152 password cipher $c$3$CRkr6IFvbGrUgoWHuUCYfSf3XLYWbQ==
 peer 200.1.15.153 as-number 100
 peer 200.1.15.153 connect-interface LoopBack0
```

```
 peer 200.1.15.153 password cipher $c$3$NzsdiaPMbqkfL5DJsga/5QHtP+w5tg==
 #
 address-family l2vpn evpn
  peer 200.1.15.152 enable
  peer 200.1.15.153 enable
```

- Main overlay configuration on leaf node Device C:

```
#
ip vpn-instance neutron-1017
 route-distinguisher 4227879168:1017
 description d3ca707e-ce59-4682-b2d8-7151744993a2
 vpn-target 1017:1017 import-extcommunity
 vpn-target 1017:1017 1:1 export-extcommunity
#
ip vpn-instance neutron-1018
 route-distinguisher 4227879168:1018
 description a9c509ca-8ec3-4860-bb03-4a6c9eae2698
 vpn-target 1018:1018 import-extcommunity
 vpn-target 1018:1018 1:1 export-extcommunity
#
interface vsi-interface4088
ip binding vpn-instance neutron-1018
ip address 10.1.1.1 255.255.255.0   //Gateway address for VMs in VXLAN 10081
mac-address 789c-2f5f-0200
arp mode uni
distributed-gateway local
#
interface vsi-interface4089
ip binding vpn-instance neutron-1018
ip address 10.1.11.1 255.255.255.0   //Gateway address for VMs in VXLAN 10018
mac-address 789c-2f5f-0200
arp mode uni
distributed-gateway local
#
l2vpn enable
#
vsi vxlan10081
gateway vsi-interface 4088

arp suppression enable
flooding disable all
vxlan 10081
evpn encapsulation vxlan         //Create an EVPN instance, and enable auto
generation of RDs and RTs for the EVPN instance
route-distinguisher auto
vpn-target auto export-extcommunity
vpn-target auto import-extcommunity
```

```
#
vsi vxlan10018
gateway vsi-interface 4089
arp suppression enable
flooding disable all
vxlan 10018
evpn encapsulation vxlan         //Create an EVPN instance, and enable auto
generation of RDs and RTs for the EVPN instance
route-distinguisher auto
vpn-target auto export-extcommunity
vpn-target auto import-extcommunity
#
```

- Main AC interface configuration on leaf node Device C:

```
#
interface Ten-GigabieEthernet1/0/5
port link-mode bridge
lldp compliance admin-status cdp txrx
service-instance 100
encapsulation s-vid 4088
xconnect vsi vxlan10018
service-instance 101
encapsulation s-vid 4089
xconnect vsi vxlan10081
#
```

Contents

Introduction

This document provides NetStream configuration examples.

Prerequisites

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of NetStream.

Restrictions and guidelines

This feature is only supported on a device installed with an H3C LSWM2FPGA or LSWM2FPGAB NetStream interface module.

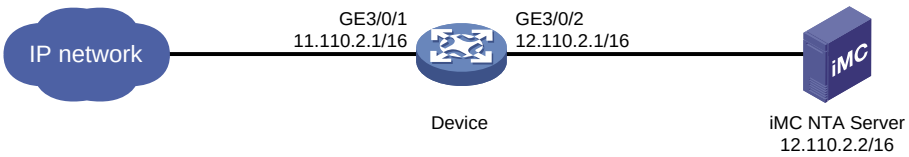
Example: Configuring NetStream

Network configuration

As shown in Figure 1, configure NetStream on the device to collect and export traffic statistics as follows:

- Export the collected traffic statistics to the IMC server with IP address 12.110.2.2/16 and UDP port 6343.
- Randomly capture one packet out of every 256 packets (both inbound and outbound) for NetStream traffic statistics collection on GigabitEthernet 3/0/1.

Figure 1 Network diagram



Analysis

To ensure that the device and the IMC server can communicate with each other, add the device to IMC NTA with the correct SNMP community string and port number.

To collect bidirectional traffic statistics on GigabitEthernet 3/0/1 of the device, enable NetStream for both the inbound and outbound traffic on GigabitEthernet 3/0/1. Specify a sampler to implement sampled-NetStream as required.

For the IMC server to analyze the NetStream statistics and generate reports based on the statistics, configure a traffic analysis task in IMC NTA.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Not supported
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Not supported
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Not supported
S6520X-SI switch series S6520-SI switch series	Not supported
S5000-EI switch series	Not supported
MS4600 switch series	Not supported
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported

Hardware	Software version
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
S5135S-EI switch series	Not supported

Restrictions and guidelines

For the device to send NetStream statistics to the IMC server, specify the IMC server with IP address 12.110.2.2/16 and UDP port 6343 as the destination host for NetStream data export.

Procedures

Configuring a NetStream interface module to work in NetStream mode

About this task

You can install a NetStream interface module on the device to provide the NetStream feature. After the device mirrors traffic to the NetStream interface module, the field programmable gate array (FPGA) chip in the module collects and analyzes traffic statistics and creates NetStream entries. This saves ACL resources and improves NetStream entry creation performance.

A NetStream interface module supports the following working modes:

- **0**—Normal mode. In this mode, NetStream is not supported.
- **1**—NetStream mode. The NetStream interface module works in the unidirectional NetStream mode.
- **2**—Session-based NetStream mode. The NetStream interface module works in the session-based bidirectional NetStream mode.

Restrictions and guidelines

To make the configuration take effect, save the configuration and reboot the device. Before you reboot the device, make sure you understand the potential impact on the network.

Procedure

1. Enter system view.

   system-view

2. Configuring a NetStream interface module to work in NetStream mode.

   fpga-working-mode slot *slot-number* **1**

   By default, a NetStream interface module works in mode 0 and the device does not support NetStream.

Configuring the device

1. Configure SNMP:

   # Enable the SNMP agent.

   ```
   <Device> system-view
   [Device] snmp-agent
   ```

   # Set the read-only community name to **public**.

   ```
   [Device] snmp-agent community read public
   ```

   # Specify the UDP port number for receiving SNMP packets as 161.

   ```
   [Device] snmp-agent port 161
   ```

2. Create sampler **256** in random sampling mode. Set the sampling rate to 8, which indicates that one packet will be randomly selected out of every 256 packets.

   ```
   [Device] sampler 256 mode random packet-interval n-power 8
   ```

3. Configure NetStream:

   # Enable NetStream sampling for both incoming and outgoing traffic on GigabitEthernet 1/0/1 with sampler **256**.

   ```
   <Device> system-view
   [Device] interface gigabitethernet 1/0/1
   ```

```
[Device-GigabitEthernet1/0/1] ip netstream inbound
[Device-GigabitEthernet1/0/1] ip netstream outbound
[Device-GigabitEthernet1/0/1] ip netstream inbound sampler 256
[Device-GigabitEthernet1/0/1] ip netstream outbound sampler 256
[Device-GigabitEthernet1/0/1] quit
```

Specify the IMC server as the NetStream data export destination.

```
[Device] ip netstream export host 12.110.2.2 6343
```

Configuring IMC

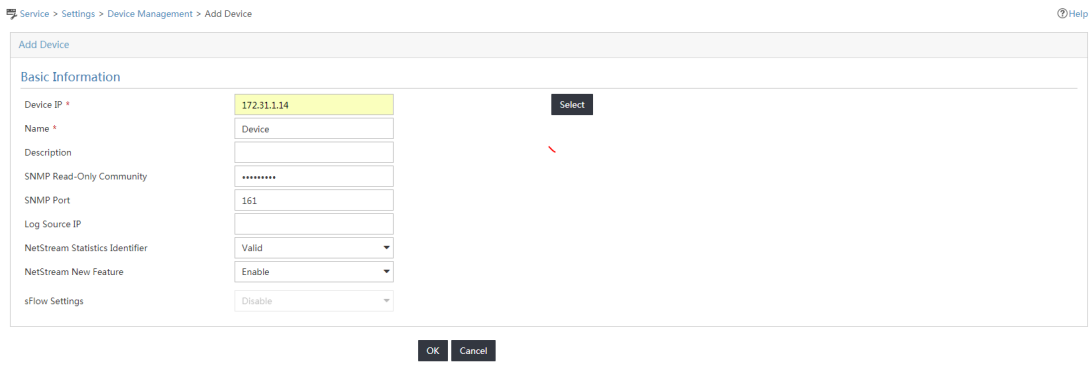
The IMC platform version running on the IMC server is PLAT 7.3 (E0504).

Adding the device to IMC NTA

1. Log in to IMC.
2. Click the **Service** tab.
3. From the left navigation pane, select **Traffic Analysis and Audit** > **Settings**.
4. On the **Settings** page that opens, click **Device Management**.

   The **Device Management** page opens.
5. Click **Add**.
6. On the **Add Device** page shown in Figure 2, perform the following steps:
   a. Enter the device IP address (12.110.2.1) in the **Device IP** field.
   b. Specify the device name, SNMP community name, SNMP port number, and other parameters as needed.
   c. Click **OK**.

Figure 2 Adding the device to IMC NTA

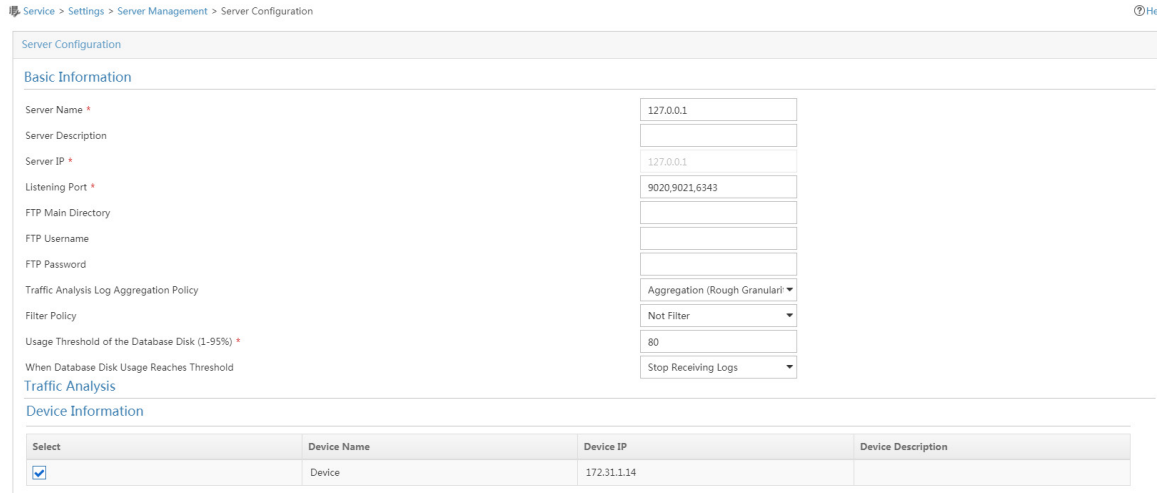


Deploying NTA server configuration to the device

1. On the **Settings** page, click **Server Management**.

   The **Server List** page opens.
2. Click the **Modify** icon for the NTA server.
3. On the **Server Configuration** page shown in Figure 3, configure the following parameters:
   a. Set port 6343 as the listening port for the server.
   b. Select the device (12.110.2.1) in the **Traffic Analysis** area.
   c. Use the default settings for the other parameters.
   d. Click **Deploy**.

Figure 3 Server Configuration



Adding a traffic analysis task

1. On the **Settings** page, click **Traffic Analysis Task Management**.

   The **Traffic Analysis Task Management** page opens.
2. Click **Add**.

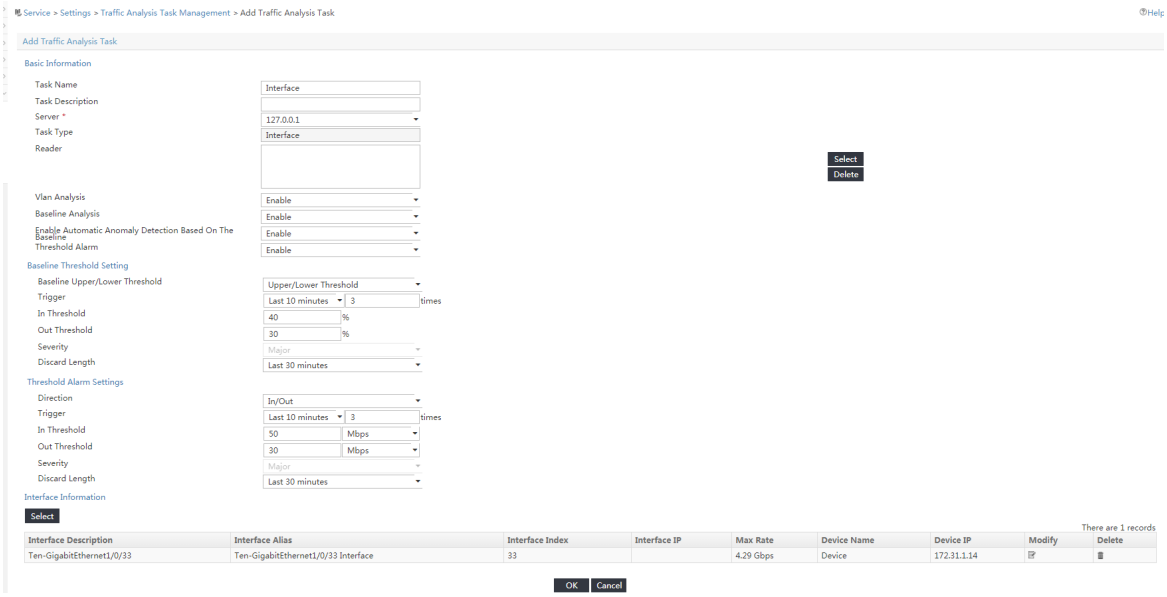
   The **Select Task Type** page opens.
3. Select **Interface** and click **Next**.

   The **Add Traffic Analysis Task** page opens.
4. In the **Basic Information** area, configure the following settings:
   - **Task Name**—Enter a task name. This example uses **Interface**.
   - **Server**—Select 127.0.0.1 from the list.
   - **Reader**—Click **Select** next to the **Reader** field, select the operator groups that have access to the analysis and reports provided by the task, and click **OK**.
   - **Vlan Analysis**—Select **Enable** from the list.
   - **Baseline Analysis**—Select **Enable** from the list.

     The **Enable Automatic Anomaly Detection Based On The Baseline** parameter and the **Baseline Threshold Setting** area are displayed.
   - **Enable Automatic Anomaly Detection Based On The Baseline**—Select **Disable** from the list.
   - **Threshold Alarm**—Select **Enable** from the list.

     The **Threshold Alarm Settings** area is displayed.
5. In the **Baseline Threshold Settings** area, set the **In Threshold** to 40% and the **Out Threshold** to 30%.
6. In the **Threshold Alarm Settings** area, set the **In Threshold** to 50 Mbps and the **Out Threshold** to 30 Mbps.
7. In the **Interface Information** area, click **Select** and select interface GigabitEthernet 1/0/2.
8. Use the default settings for the other parameters.
9. Click **OK**.

Figure 4 Adding an interface traffic analysis task



Verifying the configuration

Verifying the configuration on the device

Display NetStream data export information.

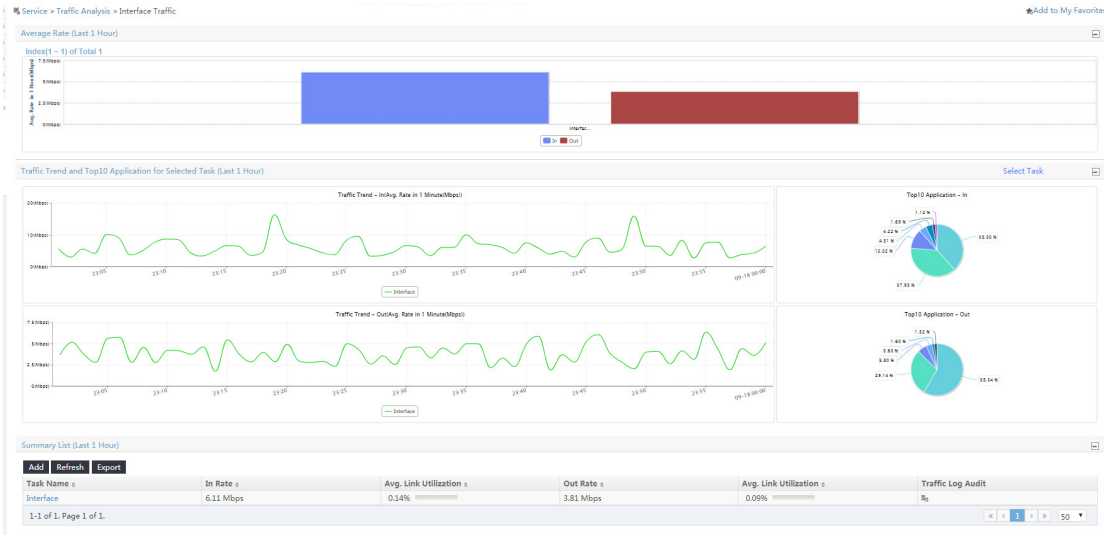
```
[Device] display ip netstream export
IP export information:
  Flow source interface                          : GigabitEthernet1/0/2
  Flow destination VPN instance                  : Not specified
  Flow destination IP address (UDP)              : 12.110.2.2 (6343)
  Version 5 exported flow number                 : 0
  Version 5 exported UDP datagram number (failed) : 0 (0)
  Version 9 exported flow number                 : 10
  Version 9 exported UDP datagram number (failed) : 10 (0)
```

Verifying the configuration on IMC

1. View the interface traffic analysis task summary reports.
   a. Click the **Service** tab.
   b. From the left navigation pane, select **Traffic Analysis and Audit** > **Interface Traffic Analysis Task**.

   The interface traffic analysis task summary reports are displayed, as shown in Figure 5.

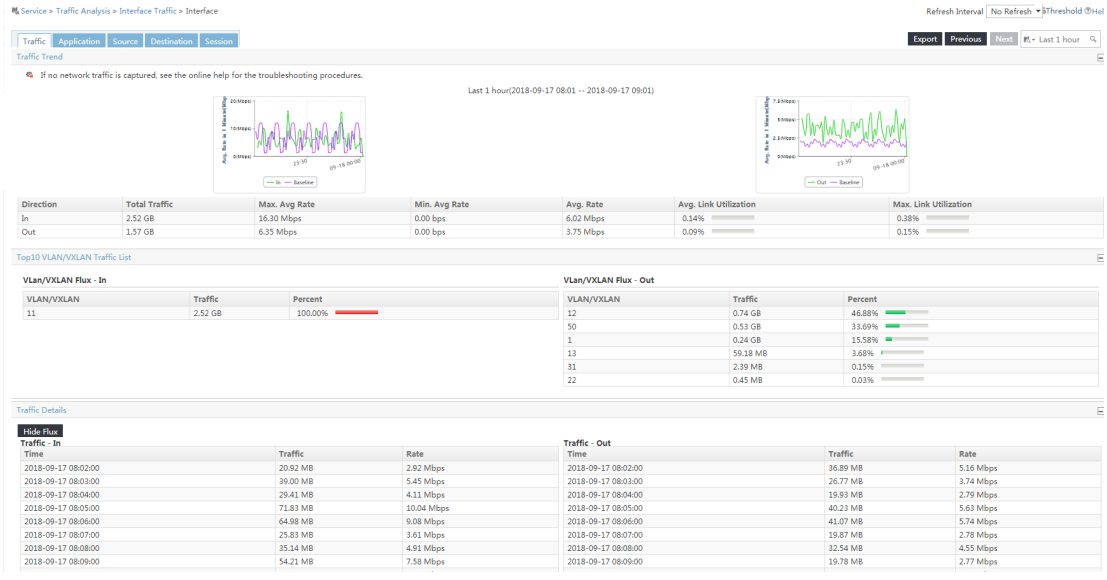
Figure 5 Summary reports for interface traffic analysis tasks



2. View detailed reports for the interface traffic analysis task named **Interface**:
   a. Click the **Service** tab.
   b. From the left navigation tree, select **Traffic Analysis and Audit** > **Interface Traffic Analysis Task**.
   c. Use either of the following methods to access the report page of interface traffic analysis task **Interface**:
      – In the **Summary List** area, click the name of interface traffic analysis task.
      – On the left navigation pane, move your mouse pointer to the shortcut menu icon >>> next to **Interface Traffic Analysis Task**, and then select **Interface** from the menu.

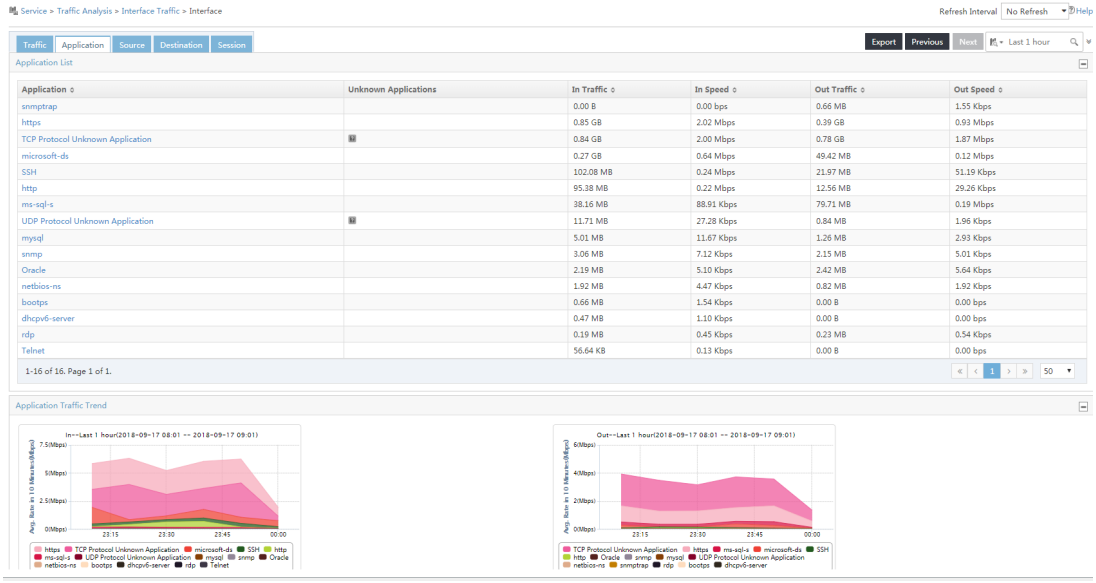
The **Traffic** tab displays the traffic analysis reports of the task.

Figure 6 Viewing the traffic analysis reports of the task



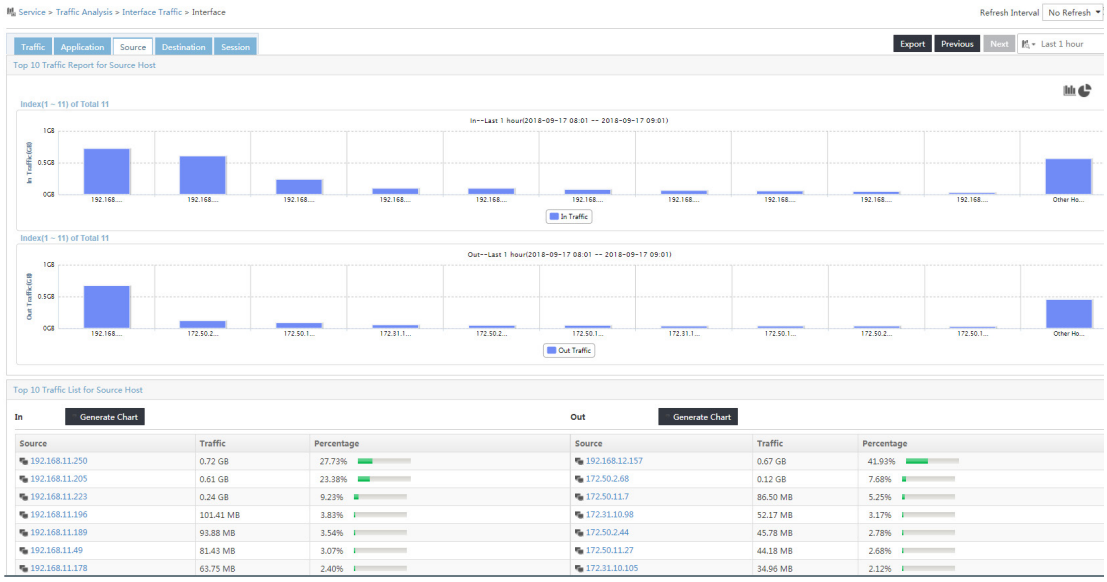
3. To view the application usage reports of the task, click the **Application** tab.

Figure 7 Viewing the application usage reports of the task



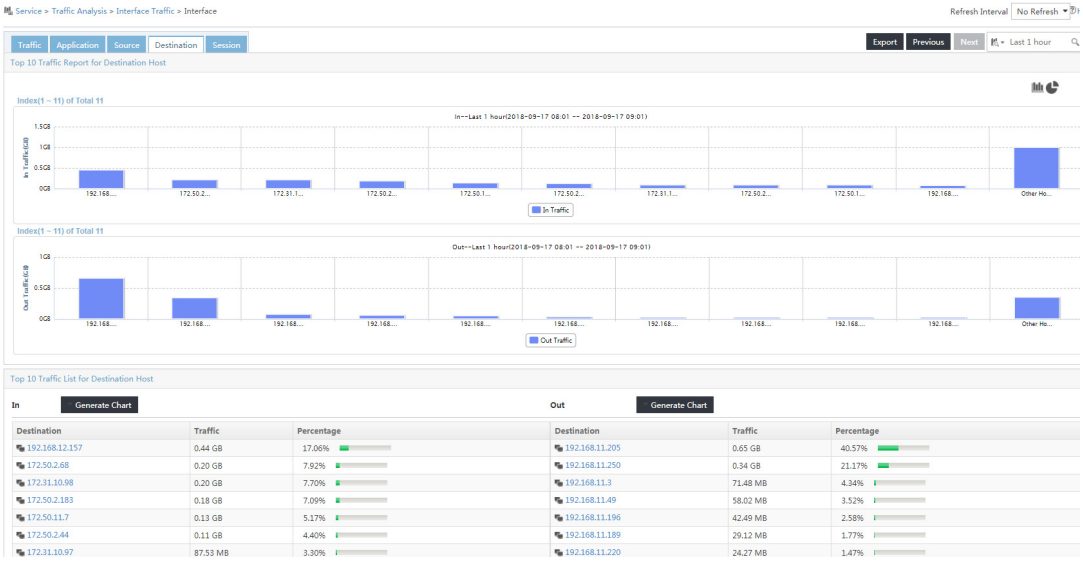
4. To view the source host-based traffic analysis reports of the task, click the **Source** tab.

Figure 8 Viewing source host-based traffic analysis reports of the task



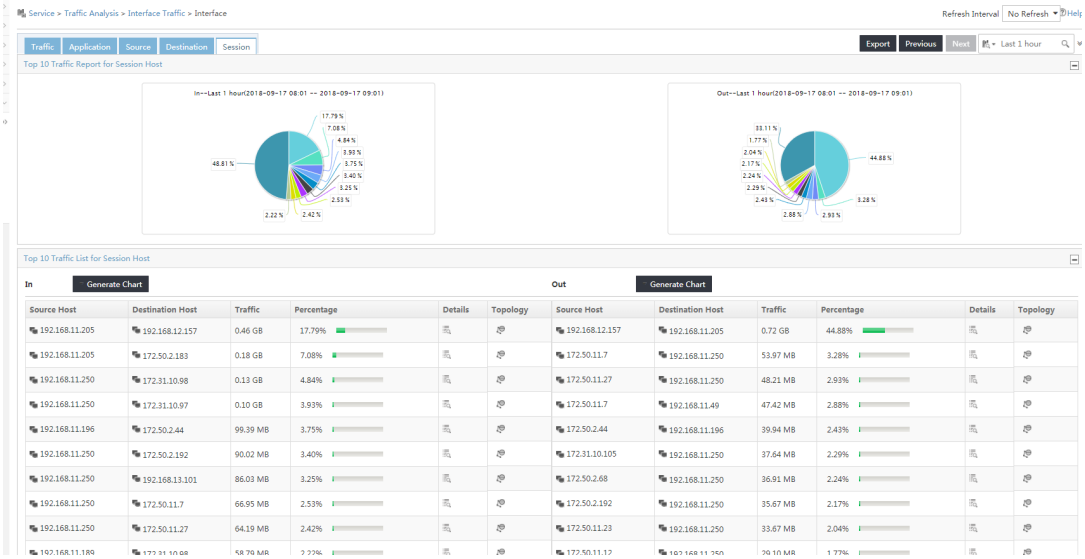
5. To view the destination host-based traffic analysis reports of the task, click the **Destination** tab.

Figure 9 Viewing destination host-based traffic analysis reports of the task



6. To view the session-based traffic analysis reports of the task, click the **Session** tab.

Figure 10 Viewing session-based traffic analysis reports of the task



Configuration files

```
#
snmp-agent
snmp-agent community read public
snmp-agent port 161
#
sampler 256 mode random packet-interval n-power 8
#
interface gigabitethernet 1/0/1
 ip address 11.110.2.1 255.255.0.0
 ip netstream inbound
```

```
 ip netstream outbound
 ip netstream inbound sampler 256
 ip netstream outbound sampler 256
#
interface gigabitethernet 1/0/2
 ip address 12.110.2.1 255.255.0.0
#
ip netstream export host 12.110.2.2 6343
#
```

Contents

Introduction

The following information provides an example for software upgrade with zero packet loss by using GIR in a VXLAN M-LAG network.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of VXLAN and GIR.

Example: Configuring software upgrade with zero packet loss by using GIR in a VXLAN M-LAG network

Network configuration

As shown in Figure 1:

- Device A and Device B act as distributed VXLAN IP gateways connected to Device E. Device A and Device B form an M-LAG system to act as a virtual VXLAN IP gateway and use a directly connected link as the peer link. Device E belongs to VXLAN 10.
- Device C and Device D act as distributed VXLAN IP gateways connected to Device F. Device C and Device D form an M-LAG system to act as a virtual VXLAN IP gateway and use a directly connected link as the peer link. Device F belongs to VXLAN 20.
- Configure Device B to enter maintenance mode and switch traffic to Device A. After Device B completes its upgrade, switch traffic back to Device B and then upgrade Device A.
- Configure Device D to enter maintenance mode and switch traffic to Device C. After Device D completes its upgrade, switch traffic back to Device D and then upgrade Device C.

Figure 1 Network diagram

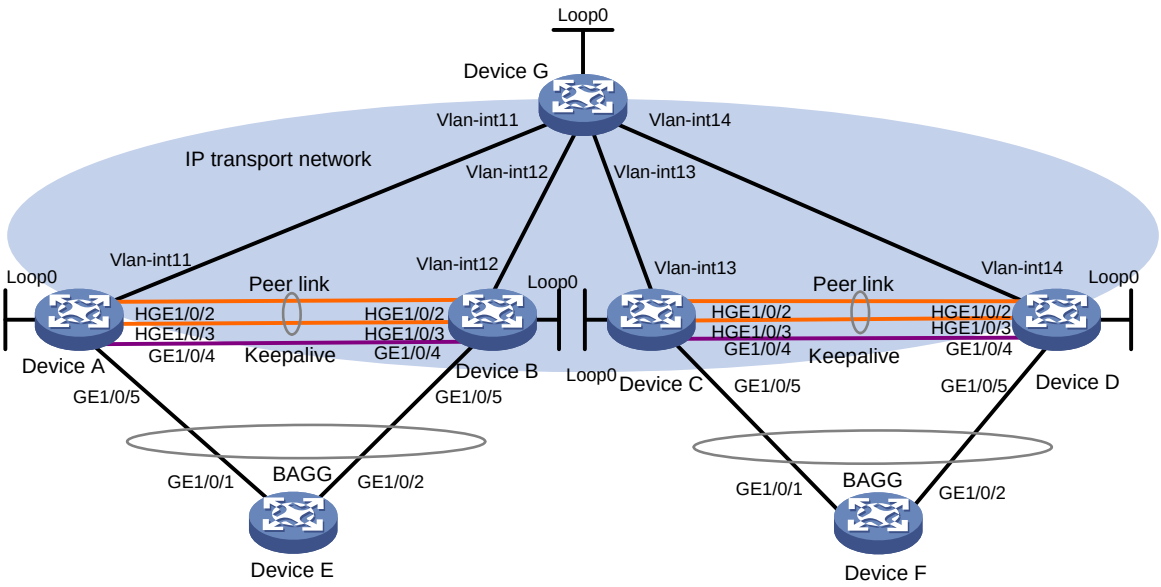


Table 1 Data plan

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-interface11	11.1.1.1/24	Device C	Vlan-interface13	13.1.1.1/24
	GE1/0/4	60.1.1.1/24		GE1/0/4	60.2.1.1/24
	Loop0	1.1.1.1/32		Loop0	2.2.2.2/32
Device B	Vlan-interface12	12.1.1.1/24	Device D	Vlan-interface14	14.1.1.1/24
	GE1/0/4	60.1.1.2/24		GE1/0/4	60.2.1.2/24
	Loop0	1.1.1.1/32		Loop0	2.2.2.2/32
Device G	Vlan-interface11	11.1.1.3/24	vpna	Vsi-interface1	10.1.1.1/24
	Vlan-interface12	12.1.1.3/24			
	Vlan-interface13	13.1.1.3/24	vpnb	Vsi-interface2	20.1.1.1/24
	Vlan-interface14	14.1.1.3/24			
	Loop0	3.3.3.3/24			

Analysis

- Device A and Device B form one M-LAG system. Device C and Device D form another M-LAG system.

- Configure Device A, Device B, Device C, and Device D as VTEPs and configure Device E as the core device.
- First use GIR to isolate and upgrade the secondary device (Device B), and then use GIR to isolate and upgrade the primary device (Device A).
- First use GIR to isolate and upgrade the secondary device (Device D), and then use GIR to isolate and upgrade the primary device (Device C).

Applicable hardware and software versions

Table 2 Applicable hardware and software versions

Product	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Release 8106Pxx
S6525XE-HI switch series	Release 8106Pxx
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Not supported
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (excluding the S5500V3-24P-SI and S5500V3-48P-SI switches)	Not supported
S5170-EI switch series	Not supported

Product	Software version
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series S5120V2-LI switch series	Not supported
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (excluding the S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI switches)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC & IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported

Product	Software version
IE4520 switch series	Not supported
S5135S-EI switch	Not supported

Restrictions and guidelines

When using GIR to upgrade or replace devices in an M-LAG network, follow these restrictions and guidelines:

- As a best practice, do not configure isolation separately for route and aggregation services to avoid issues like packet loss due to configuration omissions.
- When specifying the next startup configuration file, include maintenance mode settings in the file.

Procedures

Configuring IPv4 VXLAN M-LAG

1. Configure IP addresses and unicast routing protocols:

Configure the IP address and subnet mask for each interface. (Details not shown.)

Configure routes on the IP transport network to advertise routes for subnets attached to the interfaces (including Loopback interfaces) on each node. Make sure the devices have connectivity to each other. (Details not shown.)

2. Configure Device A:

Enable Layer 2 VPN (L2VPN).

```
<DeviceA> system-view
[DeviceA] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the peer link, with in one of the following methods. You must configure Device A and Device B in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the peer link based on VXLAN IDs.

  ```
  [DeviceA] l2vpn m-lag peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the peer link based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Set the M-LAG system number.

```
[DeviceA] m-lag system-mac 1-1-1
[DeviceA] m-lag system-number 1
[DeviceA] m-lag system-priority 10
```

```
[DeviceA] m-lag keepalive ip destination 60.1.1.2 source 60.1.1.1
[DeviceA] m-lag restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] quit
```

Assign HundredGigE1/0/2 and HundredGigE1/0/3 to aggregation group 2.

```
[DeviceA] interface HundredGigE 1/0/2
[DeviceA-HundredGigE1/0/2] port link-aggregation group 2
[DeviceA-HundredGigE1/0/2] quit
[DeviceA] interface HundredGigE 1/0/3
[DeviceA-HundredGigE1/0/3] port link-aggregation group 2
[DeviceA-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 2 to operate in dynamic aggregation mode as a peer-link interface.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] port m-lag peer-link 1
[DeviceA-Bridge-Aggregation2] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 3, and configure it as M-LAG interface 3.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] port m-lag group 3
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet1/0/5 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/5] quit
```

Create VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 3 as a trunk port and assign it to VLAN 2.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port link-type trunk
[DeviceA-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceA-Bridge-Aggregation3] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] vxlan 10
[DeviceA-vsi-vpna-vxlan-10] quit
[DeviceA-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceA] vsi vpnb
```

```
[DeviceA-vsi-vpnb] vxlan 20
[DeviceA-vsi-vpnb-vxlan-20] quit
[DeviceA-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceA] interface loopback 0
[DeviceA-Loopback0] ip address 1.1.1.1 255.255.255.255
[DeviceA-Loopback0] quit
```

Establish a VXLAN tunnel from Device A to Device C and Device D.

```
[DeviceA] interface tunnel 1 mode vxlan
[DeviceA-Tunnel1] source 1.1.1.1
[DeviceA-Tunnel1] destination 2.2.2.2
[DeviceA-Tunnel1] quit
```

Associate interface **Tunnel1** with VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] vxlan 10
[DeviceA-vsi-vpna-vxlan-10] tunnel 1
[DeviceA-vsi-vpna-vxlan-10] quit
[DeviceA-vsi-vpna] quit
```

Associate interface **Tunnel1** with VXLAN 20.

```
[DeviceA] vsi vpnb
[DeviceA-vsi-vpnb] vxlan 20
[DeviceA-vsi-vpnb-vxlan-20] tunnel 1
[DeviceA-vsi-vpnb-vxlan-20] quit
[DeviceA-vsi-vpnb] quit
```

Create Ethernet service instance 1000 on Bridge-Aggregation 3, which is connected to Device E. Configure the Ethernet service instance to match frames with outer VLAN tag 2.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] service-instance 1000
[DeviceA-Bridge-Aggregation3-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[DeviceA-Bridge-Aggregation3-srv1000] xconnect vsi vpna
[DeviceA-Bridge-Aggregation3-srv1000] quit
[DeviceA-Bridge-Aggregation3] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceA] interface vsi-interface 1
[DeviceA-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceA-Vsi-interface1] mac-address 1-1-1
[DeviceA-Vsi-interface1] distributed-gateway local
[DeviceA-Vsi-interface1] local-proxy-arp enable
[DeviceA-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceA] interface vsi-interface 2
[DeviceA-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceA-Vsi-interface2] mac-address 2-2-2
[DeviceA-Vsi-interface2] distributed-gateway local
[DeviceA-Vsi-interface2] local-proxy-arp enable
[DeviceA-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceA] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] gateway vsi-interface 1
[DeviceA-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceA] vsi vpnb
[DeviceA-vsi-vpnb] gateway vsi-interface 2
[DeviceA-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceA] m-lag mad exclude interface loopback 0
[DeviceA] m-lag mad exclude interface gigabitethernet 1/0/4
[DeviceA] m-lag mad exclude interface vsi-interface 1
[DeviceA] m-lag mad exclude interface vsi-interface 2
[DeviceA] m-lag mad exclude interface vlan-interface 11
```

3. Configure Device B:

Enable Layer 2 VPN (L2VPN).

```
<DeviceB> system-view
[DeviceB] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the peer link, with in one of the following methods. You must configure Device A and Device B in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the peer link based on VXLAN IDs.

  ```
  [DeviceB] l2vpn m-lag peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the peer link based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Set the M-LAG system number.

```
[DeviceB] m-lag system-mac 1-1-1
[DeviceB] m-lag system-number 2
[DeviceB] m-lag system-priority 10
[DeviceB] m-lag keepalive ip destination 60.1.1.1 source 60.1.1.2
[DeviceB] m-lag restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 2.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] quit
```

Assign HundredGigE1/0/2 and HundredGigE1/0/3 to aggregation group 2.

```
[DeviceB] interface HundredGigE 1/0/2
[DeviceB-HundredGigE1/0/2] port link-aggregation group 2
[DeviceB-HundredGigE1/0/2] quit
[DeviceB] interface HundredGigE 1/0/3
[DeviceB-HundredGigE1/0/3] port link-aggregation group 2
[DeviceB-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 2 to operate in dynamic aggregation mode as a peer-link interface.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation2] port m-lag peer-link 1
[DeviceB-Bridge-Aggregation2] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 3, and configure it as M-LAG interface 3.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] port m-lag group 3
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet1/0/5 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/5] quit
```

Create VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 3 as a trunk port and assign it to VLAN 2.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] port link-type trunk
[DeviceB-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceB-Bridge-Aggregation3] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] vxlan 10
[DeviceB-vsi-vpna-vxlan-10] quit
[DeviceB-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] vxlan 20
[DeviceB-vsi-vpnb-vxlan-20] quit
```

```
[DeviceB-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceB] interface loopback 0
[DeviceB-Loopback0] ip address 1.1.1.1 255.255.255.255
[DeviceB-Loopback0] quit
```

Establish a VXLAN tunnel from Device B to Device C and Device D.

```
[DeviceB] interface tunnel 1 mode vxlan
[DeviceB-Tunnel1] source 1.1.1.1
[DeviceB-Tunnel1] destination 2.2.2.2
[DeviceB-Tunnel1] quit
```

Associate interface **Tunnel1** with VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] vxlan 10
[DeviceB-vsi-vpna-vxlan-10] tunnel 1
[DeviceB-vsi-vpna-vxlan-10] quit
[DeviceB-vsi-vpna] quit
```

Associate interface **Tunnel1** with VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] vxlan 20
[DeviceB-vsi-vpnb-vxlan-20] tunnel 1
[DeviceB-vsi-vpnb-vxlan-20] quit
[DeviceB-vsi-vpnb] quit
```

Create Ethernet service instance 1000 on Bridge-Aggregation 3, which is connected to Device E. Configure the Ethernet service instance to match frames with outer VLAN tag 2.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] service-instance 1000
[DeviceB-Bridge-Aggregation3-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[DeviceB-Bridge-Aggregation3-srv1000] xconnect vsi vpna
[DeviceB-Bridge-Aggregation3-srv1000] quit
[DeviceB-Bridge-Aggregation3] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceB] interface vsi-interface 1
[DeviceB-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceB-Vsi-interface1] mac-address 1-1-1
[DeviceB-Vsi-interface1] distributed-gateway local
[DeviceB-Vsi-interface1] local-proxy-arp enable
[DeviceB-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceB] interface vsi-interface 2
[DeviceB-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceB-Vsi-interface2] mac-address 2-2-2
[DeviceB-Vsi-interface2] distributed-gateway local
[DeviceB-Vsi-interface2] local-proxy-arp enable
[DeviceB-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceB] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] gateway vsi-interface 1
[DeviceB-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] gateway vsi-interface 2
[DeviceB-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceB] m-lag mad exclude interface loopback 0
[DeviceB] m-lag mad exclude interface gigabitethernet 1/0/4
[DeviceB] m-lag mad exclude interface vsi-interface 1
[DeviceB] m-lag mad exclude interface vsi-interface 2
[DeviceB] m-lag mad exclude interface vlan-interface 12
```

4. Configure Device C:

Enable Layer 2 VPN (L2VPN).

```
<DeviceC> system-view
[DeviceC] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the peer link, with in one of the following methods. You must configure Device C and Device D in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the peer link based on VXLAN IDs.

  ```
  [DeviceC] l2vpn m-lag peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the peer link based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Set the M-LAG system number.

```
[DeviceC] m-lag system-mac 2-2-2
[DeviceC] m-lag system-number 1
[DeviceC] m-lag system-priority 10
[DeviceC] m-lag keepalive ip destination 60.2.1.2 source 60.2.1.1
[DeviceC] m-lag restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 4.

```
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] quit
```

Assign HundredGigE1/0/2 and HundredGigE1/0/3 to aggregation group 4.

```
[DeviceC] interface HundredGigE 1/0/2
[DeviceC-HundredGigE1/0/2] port link-aggregation group 4
[DeviceC-HundredGigE1/0/2] quit
[DeviceC] interface HundredGigE 1/0/3
[DeviceC-HundredGigE1/0/3] port link-aggregation group 4
[DeviceC-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 4 to operate in dynamic aggregation mode as a peer-link interface.

```
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation4] port m-lag peer-link 1
[DeviceC-Bridge-Aggregation4] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 5, and configure it as M-LAG interface 4.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation5] port m-lag group 4
[DeviceC-Bridge-Aggregation5] quit
```

Assign GigabitEthernet1/0/5 to aggregation group 5.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-aggregation group 5
[DeviceC-GigabitEthernet1/0/5] quit
```

Create VLAN 3.

```
[DeviceC] vlan 3
[DeviceC-vlan3] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 5 as a trunk port and assign it to VLAN 3.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] port link-type trunk
[DeviceC-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceC-Bridge-Aggregation5] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] vxlan 10
[DeviceC-vsi-vpna-vxlan-10] quit
[DeviceC-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] vxlan 20
[DeviceC-vsi-vpnb-vxlan-20] quit
[DeviceC-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceC] interface loopback 0
[DeviceC-Loopback0] ip address 2.2.2.2 255.255.255.255
[DeviceC-Loopback0] quit
```

Establish a VXLAN tunnel from Device C to Device A and Device B.

```
[DeviceC] interface tunnel 1 mode vxlan
[DeviceC-Tunnel1] source 2.2.2.2
[DeviceC-Tunnel1] destination 1.1.1.1
[DeviceC-Tunnel1] quit
```

Associate interface **Tunnel1** with VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] vxlan 10
[DeviceC-vsi-vpna-vxlan-10] tunnel 1
[DeviceC-vsi-vpna-vxlan-10] quit
[DeviceC-vsi-vpna] quit
```

Associate interface **Tunnel1** with VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] vxlan 20
[DeviceC-vsi-vpnb-vxlan-20] tunnel 1
[DeviceC-vsi-vpnb-vxlan-20] quit
[DeviceC-vsi-vpnb] quit
```

Create Ethernet service instance 2000 on Bridge-Aggregation 5, which is connected to Device F. Configure the Ethernet service instance to match frames with outer VLAN tag 3.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] service-instance 2000
[DeviceC-Bridge-Aggregation5-srv2000] encapsulation s-vid 3
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[DeviceC-Bridge-Aggregation5-srv2000] xconnect vsi vpnb
[DeviceC-Bridge-Aggregation5-srv2000] quit
[DeviceC-Bridge-Aggregation5] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceC] interface vsi-interface 1
[DeviceC-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceC-Vsi-interface1] mac-address 1-1-1
[DeviceC-Vsi-interface1] distributed-gateway local
[DeviceC-Vsi-interface1] local-proxy-arp enable
[DeviceC-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceC] interface vsi-interface 2
[DeviceC-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceC-Vsi-interface2] mac-address 2-2-2
[DeviceC-Vsi-interface2] distributed-gateway local
```

```
[DeviceC-Vsi-interface2] local-proxy-arp enable
[DeviceC-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceC] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] gateway vsi-interface 1
[DeviceC-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] gateway vsi-interface 2
[DeviceC-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceC] m-lag mad exclude interface loopback 0
[DeviceC] m-lag mad exclude interface gigabitethernet 1/0/4
[DeviceC] m-lag mad exclude interface vsi-interface 1
[DeviceC] m-lag mad exclude interface vsi-interface 2
[DeviceC] m-lag mad exclude interface vlan-interface 13
```

5. Configure Device D:

Enable Layer 2 VPN (L2VPN).

```
<DeviceD> system-view
[DeviceD] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the peer link, with in one of the following methods. You must configure Device C and Device D in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the peer link based on VXLAN IDs.

  ```
  [DeviceD] l2vpn m-lag peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the peer link based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Set the M-LAG system number.

```
[DeviceD] m-lag system-mac 2-2-2
[DeviceD] m-lag system-number 2
[DeviceD] m-lag system-priority 10
[DeviceD] m-lag keepalive ip destination 60.2.1.1 source 60.2.1.2
[DeviceD] m-lag restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 4.

```
[DeviceD] interface bridge-aggregation 4
[DeviceD-Bridge-Aggregation4] quit
```

Assign HundredGigE1/0/2 and HundredGigE1/0/3 to aggregation group 4.

```
[DeviceD] interface HundredGigE 1/0/2
[DeviceD-HundredGigE1/0/2] port link-aggregation group 4
[DeviceD-HundredGigE1/0/2] quit
```

```
[DeviceD] interface HundredGigE 1/0/3
[DeviceD-HundredGigE1/0/3] port link-aggregation group 4
[DeviceD-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 4 to operate in dynamic aggregation mode as a peer-link interface.

```
[DeviceD] interface bridge-aggregation 4
[DeviceD-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation4] port m-lag peer-link 1
[DeviceD-Bridge-Aggregation4] quit
```

Create dynamic Layer 2 dynamic aggregate interface Bridge-Aggregation 5, and configure it as M-LAG interface 4.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation5] port m-lag group 5
[DeviceD-Bridge-Aggregation5] quit
```

Assign GigabitEthernet1/0/5 to aggregation group 5.

```
[DeviceD] interface gigabitethernet 1/0/5
[DeviceD-GigabitEthernet1/0/5] port link-aggregation group 6
[DeviceD-GigabitEthernet1/0/5] quit
```

Create VLAN 3.

```
[DeviceD] vlan 3
[DeviceD-vlan3] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 5 as a trunk port and assign it to VLAN 3.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] port link-type trunk
[DeviceD-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceD-Bridge-Aggregation5] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] vxlan 10
[DeviceD-vsi-vpna-vxlan-10] quit
[DeviceD-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] vxlan 20
[DeviceD-vsi-vpnb-vxlan-20] quit
[DeviceD-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceD] interface loopback 0
[DeviceD-Loopback0] ip address 2.2.2.2 255.255.255.255
[DeviceD-Loopback0] quit
```

Establish a VXLAN tunnel from Device D to Device A and Device B.

```
[DeviceD] interface tunnel 1 mode vxlan
[DeviceD-Tunnel1] source 2.2.2.2
[DeviceD-Tunnel1] destination 1.1.1.1
[DeviceD-Tunnel1] quit
```

Associate interface **Tunnel1** with VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] vxlan 10
[DeviceD-vsi-vpna-vxlan-10] tunnel 1
[DeviceD-vsi-vpna-vxlan-10] quit
[DeviceD-vsi-vpna] quit
```

Associate interface **Tunnel1** with VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] vxlan 20
[DeviceD-vsi-vpnb-vxlan-20] tunnel 1
[DeviceD-vsi-vpnb-vxlan-20] quit
[DeviceD-vsi-vpnb] quit
```

Create Ethernet service instance 2000 on Bridge-Aggregation 5, which is connected to Device F. Configure the Ethernet service instance to match frames with outer VLAN tag 3.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] service-instance 2000
[DeviceD-Bridge-Aggregation5-srv2000] encapsulation s-vid 3
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[DeviceD-Bridge-Aggregation5-srv2000] xconnect vsi vpnb
[DeviceD-Bridge-Aggregation5-srv2000] quit
[DeviceD-Bridge-Aggregation5] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceD] interface vsi-interface 1
[DeviceD-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceD-Vsi-interface1] mac-address 1-1-1
[DeviceD-Vsi-interface1] distributed-gateway local
[DeviceD-Vsi-interface1] local-proxy-arp enable
[DeviceD-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceD] interface vsi-interface 2
[DeviceD-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceD-Vsi-interface2] mac-address 2-2-2
[DeviceD-Vsi-interface2] distributed-gateway local
[DeviceD-Vsi-interface2] local-proxy-arp enable
[DeviceD-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceD] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] gateway vsi-interface 1
[DeviceD-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] gateway vsi-interface 2
[DeviceD-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceD] m-lag mad exclude interface loopback 0
[DeviceD] m-lag mad exclude interface gigabitethernet 1/0/4
[DeviceD] m-lag mad exclude interface vsi-interface 1
[DeviceD] m-lag mad exclude interface vsi-interface 2
[DeviceD] m-lag mad exclude interface vlan-interface 14
```

6. Configure Device E:

Create Layer 2 aggregate interface Bridge-Aggregation 3 and configure the interface to operate in dynamic mode.

```
<DeviceE> system-view
[DeviceE] interface bridge-aggregation 3
[DeviceE-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceE-Bridge-Aggregation3] quit
```

Assign GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to aggregation group 3.

```
[DeviceE] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceE-if-range] port link-aggregation group 3
[DeviceE-if-range] quit
```

Create VLAN 2.

```
[DeviceE] vlan 2
[DeviceE-vlan2] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 3 as a trunk port and assign it to VLAN 2.

```
[DeviceE] interface bridge-aggregation 3
[DeviceE-Bridge-Aggregation3] port link-type trunk
[DeviceE-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceE-Bridge-Aggregation3] quit
```

Create VLAN-interface 2 and assign it an IP address.

```
[DeviceE] interface vlan-interface 2
[DeviceE-vlan-interface2] ip address 10.1.1.100 24
[DeviceE-vlan-interface2] quit
```

7. Configure Device F:

Create Layer 2 aggregate interface Bridge-Aggregation 5 and configure the interface to operate in dynamic mode.

```
<DeviceF> system-view
[DeviceF] interface bridge-aggregation 5
[DeviceF-Bridge-Aggregation5] link-aggregation mode dynamic
```

```
[DeviceF-Bridge-Aggregation5] quit
```

Assign GigabitEthernet1/0/1 and GigabitEthernet1/0/2 to aggregation group 5.

```
[DeviceF] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceF-if-range] port link-aggregation group 5
[DeviceF-if-range] quit
```

Create VLAN 3.

```
[DeviceF] vlan 3
[DeviceF-vlan3] quit
```

Configure Layer 2 aggregate interface Bridge-Aggregation 5 as a trunk port and assign it to VLAN 3.

```
[DeviceF] interface bridge-aggregation 5
[DeviceF-Bridge-Aggregation5] port link-type trunk
[DeviceF-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceF-Bridge-Aggregation5] quit
```

Create VLAN-interface 3 and assign it an IP address.

```
[DeviceF] interface vlan-interface 3
[DeviceF-vlan-interface3] ip address 20.1.1.100 24
[DeviceF-vlan-interface3] quit
```

Using GIR to upgrade or replace M-LAG member devices

Upgrading the secondary device (Device B)

1. Configure the maintenance mode and switch traffic to the primary device:

   # Configure the secondary device (Device B) to enter maintenance mode. Related route and aggregation settings will be automatically isolated to switch traffic to the primary device (Device A).

```
<DeviceB> system-view
[DeviceB] gir system-mode maintenance
Collecting commands... Please wait.
Configuration to be applied:
   bgp 200
     isolate enable
   isis 1
     isolate enable
   ospf 1 router-id 11.11.11.11
     isolate enable
   sleep instance 1 interval 30
   link-aggregation lacp isolate
Do you want to continue? [Y/N]: y
Generated a snapshot: before_maintenance.
Applying: bgp 200
Applying: isolate enable
Applying: isis 1
Applying: isolate enable
```

```
Applying: ospf 1 router-id 11.11.11.11
Applying: isolate enable
Applying: sleep instance 1 interval 30
Applying: link-aggregation lacp isolate
Waiting 120 seconds to release the CLI.
Changed to maintenance mode successfully.
```

Save the configuration. If you do not save the configuration, the device will be in normal mode after a successful upgrade and restart, which might result in traffic loss during switchback.

```
[DeviceB] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 6 commands and
deletes 0 commands.
If you want to see the configuration differences, please cancel this operation, and
then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Configuration is saved to device successfully.
[DeviceB] quit
```

2. Specify the upgrade file and reboot the device:

Specify the next startup configuration file.

```
<DeviceB> boot-loader file flash:/s9850_6850-f6633.ipe all main
```

(Optional.) Specify the next startup configuration file.

```
<DeviceB> startup saved-configuration flash:/m-lag_new.cfg
```

Identify whether the device will use the newly loaded image file and configuration file for the next startup.

```
<DeviceB> display boot-loader
Software images on slot 1:
Current software images:
  flash:/s9850_6850-cmw710-boot-f6632.bin
  flash:/s9850_6850-cmw710-system-f6632.bin
Main startup software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Backup startup software images:
  None
<DeviceB> display startup
MainBoard:
 Current startup saved-configuration file: flash:/m-lag_old.cfg
 Next main startup saved-configuration file: flash:/m-lag_new.cfg
 Next backup startup saved-configuration file: NULL
```

Reboot the device.

```
<DeviceB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/m-lag_old.cfg]
(To leave the existing filename unchanged, press the enter key):startup.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
```

3. Identify whether the M-LAG upgrade method is successful in maintenance mode:

Identify whether the image file has been upgraded to the target file and whether the configuration file is the target one.

```
<DeviceB> display boot-loader
Software images on slot 1:
Current software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Main startup software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Backup startup software images:
  None
<DeviceB> display startup
MainBoard:
 Current startup saved-configuration file: flash:/m-lag_new.cfg
 Next main startup saved-configuration file: flash: /m-lag_new.cfg
 Next backup startup saved-configuration file: NULL
```

Identify whether the device is operating correctly.

```
<DeviceB> display device
Slot Type               State    Subslot  Soft Ver                    Patch Ver
1    S6850-56HF         Master   0        S6850-56HF-6633             None
```

Identify whether the configuration is restored.

After startup, execute the **display current-configuration** command in any view to see the current configuration of the device. Execute the **display diff current-configuration configfile flash:/XXX.cfg** command in any view to compare the running configuration file with the one saved in the storage device and check for any lost or changed configurations.

Display the M-LAG state. The value for the **Peer-link interface state (cause)** field is **UP** when the device is operating correctly.

```
<DeviceB> display m-lag summary
Flags: A -- Aggregate interface down, B -- No peer M-LAG interface configured
       C -- Configuration consistency check failed

Peer-link interface: BAGG2
```

```
Peer-link interface state (cause): UP
Keepalive link state (cause): UP

                    M-LAG interface information
M-LAG IF    M-LAG group  Local state (cause)  Peer state  Remaining down time(s)
BAGG3       3            DOWN (A)             UP          -
```

4. Switch the traffic back to the secondary device:

   # Switch the device back to normal mode and switch the traffic to the secondary device.

```
[DeviceB] undo gir system-mode maintenance
Collecting commands... Please wait.
Configuration to be applied:
   undo link-aggregation lacp isolate
   sleep instance 1 interval 30
   ospf 1 router-id 11.11.11.11
     undo isolate enable
   isis 1
     undo isolate enable
   bgp 200
     undo isolate enable
Do you want to continue? [Y/N]: y
Applying: undo link-aggregation lacp isolate
Applying: sleep instance 1 interval 30
Applying: ospf 1 router-id 11.11.11.11
Applying: undo isolate enable
Applying: isis 1
Applying: undo isolate enable
Applying: bgp 200
Applying: undo isolate enable
Waiting 120 seconds to generate a snapshot.
Generated a snapshot: after_maintenance.
Changed to normal mode successfully.
```

5. After traffic switchback completes, identify whether the service is operating correctly:

   You can identify whether the service is operating correctly in either of the following methods:

   - Compare the collected entries (such as the routing table, FIB table, and MAC address table entries) with those before the upgrade to check for any losses. Compare the service traffic before and after the upgrade to ensure consistency.
   - Together with maintenance staff, identify whether service is operating properly and servers are operating correctly.

6. Identify whether the device is in normal mode.
7. Save the configuration. The secondary device upgrade is complete.

Upgrading the primary device (Device A)

Upgrade Device A following the steps in "Upgrading the secondary device (Device B)." (Details not shown.)

Upgrading the secondary device (Device D)

Upgrade Device D following the steps in “Upgrading the secondary device (Device B)." (Details not shown.)

Upgrading the primary device (Device C)

Upgrade Device C following the steps in "Upgrading the secondary device (Device B)." (Details not shown.)

Replacing a faulty M-LAG member device

If you need a shorter convergence time and the faulty device can be switched to maintenance mode for replacement, follow these steps to replace it:

1. Execute the **`gir system-mode maintenance`** command on the faulty device to switch the device from normal mode to maintenance mode and save the configuration.
2. Import the faulty device's configuration file to the new device.
3. Specify the image file and configuration file on the new device, and then reboot the device to apply the image file and configuration file.
4. Power off the new device or shut down all physical interfaces.
5. Shut down all physical interfaces on the faulty device or power off the faulty device. (When replacing multiple devices, power off the devices as a best practice.)
6. Replace the faulty device.
7. Connect the cables to the new device.
8. Power on the new device or bring up all physical interfaces.
9. Execute the **`undo gir system-mode maintenance`** command on the new device to switch from maintenance mode to normal mode and save the configuration.

Verifying the configuration

Verifying the configuration

1. Take Device A as an example to verify the M-LAG system configuration.

   # Display information about tunnel interfaces on Device A. The output shows that the tunnel interface in VXLAN mode is up and the tunnel source IP is 1.1.1.1.

   ```
   <DeviceA> display interface Tunnel 1
   Tunnel1
   Current state: UP
   Line protocol state: UP
   Description: Tunnel1 Interface
   Bandwidth: 64 kbps
   Maximum transmission unit: 1464
   Internet protocol processing: Disabled
   Output queue - Urgent queuing: Size/Length/Discards 0/100/0
   ```

```
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Last 300 seconds output rate: 80 bytes/sec, 640 bits/sec, 0 packets/sec
Input: 26 packets, 1974 bytes, 0 drops
Output: 340 packets, 29514 bytes, 0 drops
```

Display the VSI information on Device A. The output shows that an AC is automatically created on the peer link and associated with a VSI.

```
<DeviceA> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 1
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel1              0x5000001  UP       Manual      Disabled
  ACs:
    AC                                Link ID    State       Type
    BAGG3 srv1000                     0          Up          Manual
    BAGG2 srv2                        1          Up          Dynamic (M-LAG)

VSI Name: vpnb
  VSI Index               : 1
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
```

```
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 2
  VXLAN ID                : 20
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel1              0x5000001  UP       Manual      Disabled
```

2. Verify that hosts can access each other

   VMs Device E and Device F can access each other. If Device E disconnects from Device A or Device B, Device E and Device F can still communicate through another device.

3. Verify packet loss during an upgrade

   During the upgrade of Device A, monitor the packet loss in traffic between Device G and Device E. Empirical data shows no packet loss occurs between them.

Configuration files

- Device A:

```
#
vlan 1

#
vlan 2

#
vlan 11

#
 l2vpn enable

#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
  tunnel 1

#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
  tunnel 1

#
interface Bridge-Aggregation2
 port link-type trunk
```

```
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1

#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port m-lag group 3

#
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna

#
interface Bridge-Aggregation4

#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255

#
interface Vlan-interface2

#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0

#
interface GigabitEthernet1/0/4
 port link-mode route
 combo enable copper
 ip address 60.1.1.1 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
 combo enable copper

#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
```

```
 port link-aggregation group 3

#
interface HundredGigE1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2

#
interface HundredGigE1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2

#
interface Vsi-interface1
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local

#
interface Vsi-interface2
 ip address 20.1.1.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local

#
interface Tunnel1 mode vxlan
 source 1.1.1.1
 destination 2.2.2.2

#
 m-lag restore-delay 180
 m-lag system-mac 0001-0001-0001
 m-lag system-number 1
 m-lag system-priority 10
 m-lag keepalive ip destination 60.1.1.2 source 60.1.1.1
 m-lag mad exclude interface GigabitEthernet0/0/2
 m-lag mad exclude interface LoopBack0
 m-lag mad exclude interface Vlan-interface11
 m-lag mad exclude interface Vsi-interface1
 m-lag mad exclude interface Vsi-interface2

#
```

```
 arp distributed-gateway dynamic-entry synchronize
```

- Device B (Details not shown)
- Device C (Details not shown)
- Device D (Details not shown)
- Device E:

```
#
vlan 1

#
vlan 2

#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic

#
interface Vlan-interface2
 ip address 10.1.1.100 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
 port link-aggregation group 3

#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
 port link-aggregation group 3
```

- Device F (Details not shown)

Contents

Introduction

The following information provides an example for software upgrade with zero packet loss by using GIR in a VXLAN DRNI network.

Prerequisites

This document is not restricted to specific software or hardware versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the device.

The configuration examples were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

The following information is provided based on the assumption that you have basic knowledge of VXLAN and GIR.

Example: Configuring software upgrade with zero packet loss by using GIR in a VXLAN DRNI network

Network configuration

As shown in Figure 1:

- Device A and Device B act as distributed VXLAN IP gateways connected to Device E. Device A and Device B form a DR system to act as a virtual VXLAN IP gateway and use an Ethernet aggregate link as the IPL. Device E belongs to VXLAN 10.
- Device C and Device D act as distributed VXLAN IP gateways connected to Device F. Device C and Device D form a DR system to act as a virtual VXLAN IP gateway and use an Ethernet aggregate link as the IPL. Device F belongs to VXLAN 20.
- Configure Device B to enter maintenance mode and switch traffic to Device A. After Device B completes its upgrade, switch traffic back to Device B and then upgrade Device A.
- Configure Device D to enter maintenance mode and switch traffic to Device C. After Device D completes its upgrade, switch traffic back to Device D and then upgrade Device C.

Figure 1 Network diagram

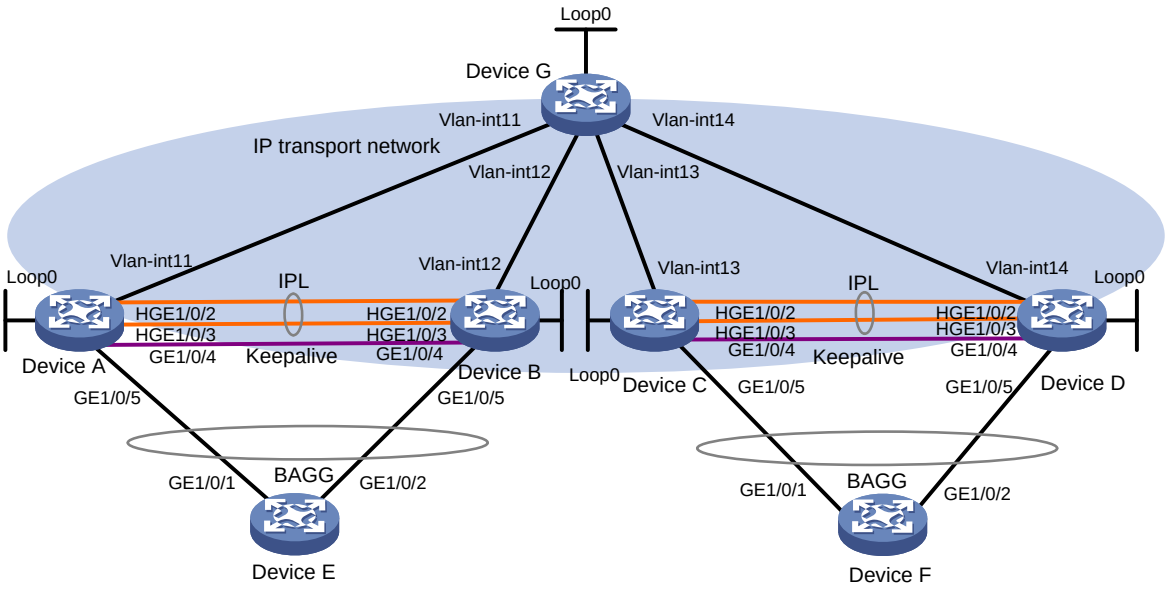


Table 1 Configuration data

Device	Interface	IP address	Device	Interface	IP address
Device A	Vlan-interface11	11.1.1.1/24	Device C	Vlan-interface13	13.1.1.1/24
	GE 1/0/4	60.1.1.1/24		GE 1/0/4	60.2.1.1/24
	Loop0	1.1.1.1/32		Loop0	2.2.2.2/32
Device B	Vlan-interface12	12.1.1.1/24	Device D	Vlan-interface14	14.1.1.1/24
	GE 1/0/4	60.1.1.2/24		GE 1/0/4	60.2.1.2/24
	Loop0	1.1.1.1/32		Loop0	2.2.2.2/32
Device G	Vlan-interface11	11.1.1.3/24	vpna	Vsi-interface1	10.1.1.1/24
	Vlan-interface12	12.1.1.3/24			
	Vlan-interface13	13.1.1.3/24	vpnb	Vsi-interface2	20.1.1.1/24
	Vlan-interface14	14.1.1.3/24			
	Loop0	3.3.3.3/24			

Analysis

To meet this requirement, perform the following tasks:

- Device A and Device B form one DR system, while Device C and Device D form another.
- Configure Device A, Device B, Device C, and Device D as VTEPs and configure Device E as the core device.
- First use GIR to isolate and upgrade the secondary device (Device B), and then use GIR to isolate and upgrade the primary device (Device A).

- First use GIR to isolate and upgrade the secondary device (Device D), and then use GIR to isolate and upgrade the primary device (Device C).

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
S6812 switch series S6813 switch series	Release 6628Pxx
S6550XE-HI switch series	Not supported
S6525XE-HI switch series	Not supported
S5850 switch series	Not supported
S5570S-EI switch series	Not supported
S5560X-EI switch series	Release 6628Pxx
S5560X-HI switch series	Release 6628Pxx
S5500V2-EI switch series	Release 6628Pxx
MS4520V2-30F switch	Release 6628Pxx
MS4520V2-30C switch MS4520V2-54C switch	Release 6628Pxx
MS4520V2-28S switch MS4520V2-24TP switch	Release 63xx
S6520X-HI switch series S6520X-EI switch series	Release 6628Pxx
S6520X-SI switch series S6520-SI switch series	Release 6628Pxx
S5000-EI switch series	Release 6628Pxx
MS4600 switch series	Release 6628Pxx
ES5500 switch series	Release 6628Pxx
S5560S-EI switch series S5560S-SI switch series	Not supported
S5500V3-24P-SI switch S5500V3-48P-SI switch	Not supported
S5500V3-SI switch series (except S5500V3-24P-SI and S5500V3-48P-SI)	Not supported
S5170-EI switch series	Not supported
S5130S-HI switch series S5130S-EI switch series S5130S-SI switch series S5130S-LI switch series	Not supported
S5120V2-SI switch series	Not supported

Hardware	Software version
S5120V2-LI switch series	
S5120V3-EI switch series	Not supported
S5120V3-36F-SI switch S5120V3-28P-HPWR-SI switch S5120V3-54P-PWR-SI switch	Not supported
S5120V3-SI switch series (except S5120V3-36F-SI, S5120V3-28P-HPWR-SI, and S5120V3-54P-PWR-SI)	Not supported
S5120V3-LI switch series	Not supported
S3600V3-EI switch series	Not supported
S3600V3-SI switch series	Not supported
S3100V3-EI switch series S3100V3-SI switch series	Not supported
S5110V2 switch series	Not supported
S5110V2-SI switch series	Not supported
S5000V3-EI switch series S5000V5-EI switch series	Not supported
S5000E-X switch series S5000X-EI switch series	Not supported
E128C switch E152C switch E500C switch series E500D switch series	Not supported
MS4320V2 switch series MS4320V3 switch series MS4300V2 switch series MS4320 switch series MS4200 switch series	Not supported
WS5850-WiNet switch series	Not supported
WS5820-WiNet switch series WS5810-WiNet switch series	Not supported
WAS6000 switch series	Not supported
IE4300-12P-AC switch IE4300-12P-PWR switch IE4300-M switch series IE4320 switch series	Not supported
IE4520 switch series	Not supported
S5135S-EI switch	Not supported

Restrictions and guidelines

When using GIR to upgrade or replace devices in a DRNI network, follow these restrictions and guidelines:

- As a best practice, do not configure isolation separately for route and aggregation services to avoid issues like packet loss due to configuration omissions.
- When specifying the next startup configuration file, include maintenance mode settings in the file.

Procedures

Configuring IPv4 VXLAN to support DRNI

1. Configure IP addresses and unicast routing protocols:

Configure the IP address and subnet mask for each interface. (Details not shown.)

Configure routes on the IP transport network to advertise routes for subnets attached to the interfaces (including Loopback interfaces) on each node. Make sure the devices have connectivity to each other. (Details not shown.)

2. Configure Device A:

Enable L2VPN.

```
<DeviceA> system-view
[DeviceA] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the IPL in one of the following methods. You must configure Device A and Device B in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the IPL based on VXLAN IDs.

  ```
  [DeviceA] l2vpn drni peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the IPL based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Configure the DR system parameters.

```
[DeviceA] drni system-mac 1-1-1
[DeviceA] drni system-number 1
[DeviceA] drni system-priority 10
[DeviceA] drni keepalive ip destination 60.1.1.2 source 60.1.1.1
[DeviceA] drni restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 2.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] quit
```

Assign HundredGigE 1/0/2 and HundredGigE 1/0/3 to aggregation group 2.

```
[DeviceA] interface HundredGigE 1/0/2
[DeviceA-HundredGigE1/0/2] port link-aggregation group 2
[DeviceA-HundredGigE1/0/2] quit
[DeviceA] interface HundredGigE 1/0/3
[DeviceA-HundredGigE1/0/3] port link-aggregation group 2
[DeviceA-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 2 to operate in dynamic aggregation mode as the IPP.

```
[DeviceA] interface bridge-aggregation 2
[DeviceA-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation2] port drni intra-portal-port 1
[DeviceA-Bridge-Aggregation2] quit
```

Create dynamic Layer 2 aggregate interface Bridge-Aggregation 3, and assign it to DR group 3.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation3] port drni group 3
[DeviceA-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/5 to aggregation group 3.

```
[DeviceA] interface gigabitethernet 1/0/5
[DeviceA-GigabitEthernet1/0/5] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/5] quit
```

Create VLAN 2.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 2.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] port link-type trunk
[DeviceA-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceA-Bridge-Aggregation3] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] vxlan 10
[DeviceA-vsi-vpna-vxlan-10] quit
[DeviceA-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceA] vsi vpnb
[DeviceA-vsi-vpnb] vxlan 20
[DeviceA-vsi-vpnb-vxlan-20] quit
[DeviceA-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceA] interface loopback 0
[DeviceA-Loopback0] ip address 1.1.1.1 255.255.255.255
[DeviceA-Loopback0] quit
```

Establish a VXLAN tunnel from Device A to Device C and Device D.

```
[DeviceA] interface tunnel 1 mode vxlan
[DeviceA-Tunnel1] source 1.1.1.1
[DeviceA-Tunnel1] destination 2.2.2.2
[DeviceA-Tunnel1] quit
```

Assign Tunnel 1 to VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] vxlan 10
[DeviceA-vsi-vpna-vxlan-10] tunnel 1
[DeviceA-vsi-vpna-vxlan-10] quit
[DeviceA-vsi-vpna] quit
```

Assign Tunnel 1 to VXLAN 20.

```
[DeviceA] vsi vpnb
[DeviceA-vsi-vpnb] vxlan 20
[DeviceA-vsi-vpnb-vxlan-20] tunnel 1
[DeviceA-vsi-vpnb-vxlan-20] quit
[DeviceA-vsi-vpnb] quit
```

Create Ethernet service instance 1000 on Bridge-Aggregation 3, which is connected to Device E. Configure the Ethernet service instance to match frames with outer VLAN tag 2.

```
[DeviceA] interface bridge-aggregation 3
[DeviceA-Bridge-Aggregation3] service-instance 1000
[DeviceA-Bridge-Aggregation3-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[DeviceA-Bridge-Aggregation3-srv1000] xconnect vsi vpna
[DeviceA-Bridge-Aggregation3-srv1000] quit
[DeviceA-Bridge-Aggregation3] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceA] interface vsi-interface 1
[DeviceA-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceA-Vsi-interface1] mac-address 1-1-1
[DeviceA-Vsi-interface1] distributed-gateway local
[DeviceA-Vsi-interface1] local-proxy-arp enable
[DeviceA-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceA] interface vsi-interface 2
[DeviceA-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceA-Vsi-interface2] mac-address 2-2-2
[DeviceA-Vsi-interface2] distributed-gateway local
[DeviceA-Vsi-interface2] local-proxy-arp enable
[DeviceA-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceA] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceA] vsi vpna
[DeviceA-vsi-vpna] gateway vsi-interface 1
[DeviceA-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceA] vsi vpnb
[DeviceA-vsi-vpnb] gateway vsi-interface 2
[DeviceA-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceA] drni mad exclude interface loopback 0
[DeviceA] drni mad exclude interface gigabitethernet 1/0/4
[DeviceA] drni mad exclude interface vsi-interface 1
[DeviceA] drni mad exclude interface vsi-interface 2
[DeviceA] drni mad exclude interface vlan-interface 11
```

3. Configure Device B:

Enable L2VPN.

```
<DeviceB> system-view
[DeviceB] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the IPL in one of the following methods. You must configure Device A and Device B in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the IPL based on VXLAN IDs.

  ```
  [DeviceB] l2vpn drni peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the IPL based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Configure the DR system parameters.

```
[DeviceB] drni system-mac 1-1-1
[DeviceB] drni system-number 2
[DeviceB] drni system-priority 10
[DeviceB] drni keepalive ip destination 60.1.1.1 source 60.1.1.2
[DeviceB] drni restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 2.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] quit
```

Assign HundredGigE 1/0/2 and HundredGigE 1/0/3 to aggregation group 2.

```
[DeviceB] interface HundredGigE 1/0/2
[DeviceB-HundredGigE1/0/2] port link-aggregation group 2
[DeviceB-HundredGigE1/0/2] quit
[DeviceB] interface HundredGigE 1/0/3
[DeviceB-HundredGigE1/0/3] port link-aggregation group 2
[DeviceB-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 2 to operate in dynamic aggregation mode as the IPP.

```
[DeviceB] interface bridge-aggregation 2
[DeviceB-Bridge-Aggregation2] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation2] port drni intra-portal-port 1
[DeviceB-Bridge-Aggregation2] quit
```

Create dynamic Layer 2 aggregate interface Bridge-Aggregation 3, and assign it to DR group 3.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceB-Bridge-Aggregation3] port drni group 3
[DeviceB-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/5 to aggregation group 3.

```
[DeviceB] interface gigabitethernet 1/0/5
[DeviceB-GigabitEthernet1/0/5] port link-aggregation group 3
[DeviceB-GigabitEthernet1/0/5] quit
```

Create VLAN 2.

```
[DeviceB] vlan 2
[DeviceB-vlan2] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 2.

```
[DeviceB] interface bridge-aggregation 3
```

```
[DeviceB-Bridge-Aggregation3] port link-type trunk
[DeviceB-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceB-Bridge-Aggregation3] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] vxlan 10
[DeviceB-vsi-vpna-vxlan-10] quit
[DeviceB-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] vxlan 20
[DeviceB-vsi-vpnb-vxlan-20] quit
[DeviceB-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceB] interface loopback 0
[DeviceB-Loopback0] ip address 1.1.1.1 255.255.255.255
[DeviceB-Loopback0] quit
```

Establish a VXLAN tunnel from Device B to Device C and Device D.

```
[DeviceB] interface tunnel 1 mode vxlan
[DeviceB-Tunnel1] source 1.1.1.1
[DeviceB-Tunnel1] destination 2.2.2.2
[DeviceB-Tunnel1] quit
```

Assign Tunnel 1 to VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] vxlan 10
[DeviceB-vsi-vpna-vxlan-10] tunnel 1
[DeviceB-vsi-vpna-vxlan-10] quit
[DeviceB-vsi-vpna] quit
```

Assign Tunnel 1 to VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] vxlan 20
[DeviceB-vsi-vpnb-vxlan-20] tunnel 1
[DeviceB-vsi-vpnb-vxlan-20] quit
[DeviceB-vsi-vpnb] quit
```

Create Ethernet service instance 1000 on Bridge-Aggregation 3, which is connected to Device E. Configure the Ethernet service instance to match frames with outer VLAN tag 2.

```
[DeviceB] interface bridge-aggregation 3
[DeviceB-Bridge-Aggregation3] service-instance 1000
[DeviceB-Bridge-Aggregation3-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[DeviceB-Bridge-Aggregation3-srv1000] xconnect vsi vpna
[DeviceB-Bridge-Aggregation3-srv1000] quit
[DeviceB-Bridge-Aggregation3] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceB] interface vsi-interface 1
```

```
[DeviceB-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceB-Vsi-interface1] mac-address 1-1-1
[DeviceB-Vsi-interface1] distributed-gateway local
[DeviceB-Vsi-interface1] local-proxy-arp enable
[DeviceB-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceB] interface vsi-interface 2
[DeviceB-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceB-Vsi-interface2] mac-address 2-2-2
[DeviceB-Vsi-interface2] distributed-gateway local
[DeviceB-Vsi-interface2] local-proxy-arp enable
[DeviceB-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceB] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceB] vsi vpna
[DeviceB-vsi-vpna] gateway vsi-interface 1
[DeviceB-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceB] vsi vpnb
[DeviceB-vsi-vpnb] gateway vsi-interface 2
[DeviceB-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceB] drni mad exclude interface loopback 0
[DeviceB] drni mad exclude interface gigabitethernet 1/0/4
[DeviceB] drni mad exclude interface vsi-interface 1
[DeviceB] drni mad exclude interface vsi-interface 2
[DeviceB] drni mad exclude interface vlan-interface 12
```

4. Configure Device C:

Enable L2VPN.

```
<DeviceC> system-view
[DeviceC] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the IPL in one of the following methods. You must configure Device C and Device D in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the IPL based on VXLAN IDs.
  ```
  [DeviceC] l2vpn drni peer-link ac-match-rule vxlan-mapping
  ```
- Method 2: Create an AC on the IPL based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Configure the DR system parameters.

```
[DeviceC] drni system-mac 2-2-2
[DeviceC] drni system-number 1
[DeviceC] drni system-priority 10
[DeviceC] drni keepalive ip destination 60.2.1.2 source 60.2.1.1
[DeviceC] drni restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 4.

```
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] quit
```

Assign HundredGigE 1/0/2 and HundredGigE 1/0/3 to aggregation group 4.

```
[DeviceC] interface HundredGigE 1/0/2
[DeviceC-HundredGigE1/0/2] port link-aggregation group 4
[DeviceC-HundredGigE1/0/2] quit
[DeviceC] interface HundredGigE 1/0/3
[DeviceC-HundredGigE1/0/3] port link-aggregation group 4
[DeviceC-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 4 to operate in dynamic aggregation mode as the IPP.

```
[DeviceC] interface bridge-aggregation 4
[DeviceC-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation4] port drni intra-portal-port 1
[DeviceC-Bridge-Aggregation4] quit
```

Create dynamic Layer 2 aggregate interface Bridge-Aggregation 5, and assign it to DR group 4.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] link-aggregation mode dynamic
[DeviceC-Bridge-Aggregation5] port drni group 4
[DeviceC-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/5 to aggregation group 5.

```
[DeviceC] interface gigabitethernet 1/0/5
[DeviceC-GigabitEthernet1/0/5] port link-aggregation group 5
[DeviceC-GigabitEthernet1/0/5] quit
```

Create VLAN 3.

```
[DeviceC] vlan 3
[DeviceC-vlan3] quit
```

Set the link type of Bridge-Aggregation 5 to trunk, and assign it to VLAN 3.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] port link-type trunk
[DeviceC-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceC-Bridge-Aggregation5] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] vxlan 10
[DeviceC-vsi-vpna-vxlan-10] quit
[DeviceC-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] vxlan 20
[DeviceC-vsi-vpnb-vxlan-20] quit
[DeviceC-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceC] interface loopback 0
[DeviceC-Loopback0] ip address 2.2.2.2 255.255.255.255
[DeviceC-Loopback0] quit
```

Establish a VXLAN tunnel from Device C to Device A and Device B.

```
[DeviceC] interface tunnel 1 mode vxlan
[DeviceC-Tunnel1] source 2.2.2.2
[DeviceC-Tunnel1] destination 1.1.1.1
[DeviceC-Tunnel1] quit
```

Assign Tunnel 1 to VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] vxlan 10
[DeviceC-vsi-vpna-vxlan-10] tunnel 1
[DeviceC-vsi-vpna-vxlan-10] quit
[DeviceC-vsi-vpna] quit
```

Assign Tunnel 1 to VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] vxlan 20
[DeviceC-vsi-vpnb-vxlan-20] tunnel 1
[DeviceC-vsi-vpnb-vxlan-20] quit
[DeviceC-vsi-vpnb] quit
```

Create Ethernet service instance 2000 on Bridge-Aggregation 5, which is connected to Device F. Configure the Ethernet service instance to match frames with outer VLAN tag 3.

```
[DeviceC] interface bridge-aggregation 5
[DeviceC-Bridge-Aggregation5] service-instance 2000
[DeviceC-Bridge-Aggregation5-srv2000] encapsulation s-vid 3
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[DeviceC-Bridge-Aggregation5-srv2000] xconnect vsi vpnb
[DeviceC-Bridge-Aggregation5-srv2000] quit
[DeviceC-Bridge-Aggregation5] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceC] interface vsi-interface 1
[DeviceC-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceC-Vsi-interface1] mac-address 1-1-1
[DeviceC-Vsi-interface1] distributed-gateway local
[DeviceC-Vsi-interface1] local-proxy-arp enable
[DeviceC-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceC] interface vsi-interface 2
[DeviceC-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceC-Vsi-interface2] mac-address 2-2-2
[DeviceC-Vsi-interface2] distributed-gateway local
[DeviceC-Vsi-interface2] local-proxy-arp enable
[DeviceC-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceC] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceC] vsi vpna
[DeviceC-vsi-vpna] gateway vsi-interface 1
```

```
[DeviceC-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceC] vsi vpnb
[DeviceC-vsi-vpnb] gateway vsi-interface 2
[DeviceC-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceC] drni mad exclude interface loopback 0
[DeviceC] drni mad exclude interface gigabitethernet 1/0/4
[DeviceC] drni mad exclude interface vsi-interface 1
[DeviceC] drni mad exclude interface vsi-interface 2
[DeviceC] drni mad exclude interface vlan-interface 13
```

5. Configure Device D:

Enable L2VPN.

```
<DeviceD> system-view
[DeviceD] l2vpn enable
```

Configure the frame match criteria for dynamic ACs on the IPL in one of the following methods. You must configure Device C and Device D in the same method.

- Method 1: Create the frame match criteria of dynamic ACs on the IPL based on VXLAN IDs.

  ```
  [DeviceD] l2vpn drni peer-link ac-match-rule vxlan-mapping
  ```

- Method 2: Create an AC on the IPL based on the frame match criteria of the site-facing Ethernet service instance.

  You do not need to configure other settings. This method is used by default.

Configure the DR system parameters.

```
[DeviceD] drni system-mac 2-2-2
[DeviceD] drni system-number 2
[DeviceD] drni system-priority 10
[DeviceD] drni keepalive ip destination 60.2.1.1 source 60.2.1.2
[DeviceD] drni restore-delay 180
```

Create Layer 2 aggregate interface Bridge-aggregation 4.

```
[DeviceD] interface bridge-aggregation 4
[DeviceD-Bridge-Aggregation4] quit
```

Assign HundredGigE 1/0/2 and HundredGigE 1/0/3 to aggregation group 4.

```
[DeviceD] interface HundredGigE 1/0/2
[DeviceD-HundredGigE1/0/2] port link-aggregation group 4
[DeviceD-HundredGigE1/0/2] quit
[DeviceD] interface HundredGigE 1/0/3
[DeviceD-HundredGigE1/0/3] port link-aggregation group 4
[DeviceD-HundredGigE1/0/3] quit
```

Configure interface Bridge-Aggregation 4 to operate in dynamic aggregation mode as the IPP.

```
[DeviceD] interface bridge-aggregation 4
[DeviceD-Bridge-Aggregation4] link-aggregation mode dynamic
[DeviceD-Bridge-Aggregation4] port drni intra-portal-port 1
[DeviceD-Bridge-Aggregation4] quit
```

Create Layer 2 dynamic aggregate interface Bridge-Aggregation 5, and assign it to DR group 4.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] link-aggregation mode dynamic
```

```
[DeviceD-Bridge-Aggregation5] port drni group 5
[DeviceD-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/5 to aggregation group 5.

```
[DeviceD] interface gigabitethernet 1/0/5
[DeviceD-GigabitEthernet1/0/5] port link-aggregation group 6
[DeviceD-GigabitEthernet1/0/5] quit
```

Create VLAN 3.

```
[DeviceD] vlan 3
[DeviceD-vlan3] quit
```

Set the link type of Bridge-Aggregation 5 to trunk, and assign it to VLAN 3.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] port link-type trunk
[DeviceD-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceD-Bridge-Aggregation5] quit
```

Create VSI instance **vpna** and VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] vxlan 10
[DeviceD-vsi-vpna-vxlan-10] quit
[DeviceD-vsi-vpna] quit
```

Create VSI instance **vpnb** and VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] vxlan 20
[DeviceD-vsi-vpnb-vxlan-20] quit
[DeviceD-vsi-vpnb] quit
```

Configure an IP address for interface Loopback0, which is to be used as the source address for the tunnel.

```
[DeviceD] interface loopback 0
[DeviceD-Loopback0] ip address 2.2.2.2 255.255.255.255
[DeviceD-Loopback0] quit
```

Establish a VXLAN tunnel from Device D to Device A and Device B.

```
[DeviceD] interface tunnel 1 mode vxlan
[DeviceD-Tunnel1] source 2.2.2.2
[DeviceD-Tunnel1] destination 1.1.1.1
[DeviceD-Tunnel1] quit
```

Assign Tunnel 1 to VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] vxlan 10
[DeviceD-vsi-vpna-vxlan-10] tunnel 1
[DeviceD-vsi-vpna-vxlan-10] quit
[DeviceD-vsi-vpna] quit
```

Assign Tunnel 1 to VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] vxlan 20
[DeviceD-vsi-vpnb-vxlan-20] tunnel 1
[DeviceD-vsi-vpnb-vxlan-20] quit
[DeviceD-vsi-vpnb] quit
```

Create Ethernet service instance 2000 on Bridge-Aggregation 5, which is connected to Device F. Configure the Ethernet service instance to match frames with outer VLAN tag 3.

```
[DeviceD] interface bridge-aggregation 5
[DeviceD-Bridge-Aggregation5] service-instance 2000
[DeviceD-Bridge-Aggregation5-srv2000] encapsulation s-vid 3
```

Map Ethernet service instance 2000 to VSI **vpnb**.

```
[DeviceD-Bridge-Aggregation5-srv2000] xconnect vsi vpnb
[DeviceD-Bridge-Aggregation5-srv2000] quit
[DeviceD-Bridge-Aggregation5] quit
```

Create VSI-interface 1, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 10. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceD] interface vsi-interface 1
[DeviceD-Vsi-interface1] ip address 10.1.1.1 255.255.255.0
[DeviceD-Vsi-interface1] mac-address 1-1-1
[DeviceD-Vsi-interface1] distributed-gateway local
[DeviceD-Vsi-interface1] local-proxy-arp enable
[DeviceD-Vsi-interface1] quit
```

Create VSI-interface 2, and assign an IP address and MAC address to it. The IP address will be used as the gateway IP address for VMs in VXLAN 20. Specify the VSI interface as a distributed gateway to provide services for the local site.

```
[DeviceD] interface vsi-interface 2
[DeviceD-Vsi-interface2] ip address 20.1.1.1 255.255.255.0
[DeviceD-Vsi-interface2] mac-address 2-2-2
[DeviceD-Vsi-interface2] distributed-gateway local
[DeviceD-Vsi-interface2] local-proxy-arp enable
[DeviceD-Vsi-interface2] quit
```

Enable dynamic ARP entry synchronization for distributed VXLAN IP gateways.

```
[DeviceD] arp distributed-gateway dynamic-entry synchronize
```

Specify VSI-interface 1 as the gateway interface for the VSI of VXLAN 10.

```
[DeviceD] vsi vpna
[DeviceD-vsi-vpna] gateway vsi-interface 1
[DeviceD-vsi-vpna] quit
```

Specify VSI-interface 2 as the gateway interface for the VSI of VXLAN 20.

```
[DeviceD] vsi vpnb
[DeviceD-vsi-vpnb] gateway vsi-interface 2
[DeviceD-vsi-vpnb] quit
```

Exclude all VXLAN interfaces from the shutdown action by M-LAG MAD.

```
[DeviceD] drni mad exclude interface loopback 0
[DeviceD] drni mad exclude interface gigabitethernet 1/0/4
[DeviceD] drni mad exclude interface vsi-interface 1
[DeviceD] drni mad exclude interface vsi-interface 2
[DeviceD] drni mad exclude interface vlan-interface 14
```

6. Configure Device E:

Create Layer 2 aggregate interface Bridge-Aggregation 3 and configure the interface to operate in dynamic mode.

```
<DeviceE> system-view
[DeviceE] interface bridge-aggregation 3
[DeviceE-Bridge-Aggregation3] link-aggregation mode dynamic
[DeviceE-Bridge-Aggregation3] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 3.

```
[DeviceE] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceE-if-range] port link-aggregation group 3
[DeviceE-if-range] quit
```

Create VLAN 2.

```
[DeviceE] vlan 2
[DeviceE-vlan2] quit
```

Set the link type of Bridge-Aggregation 3 to trunk, and assign it to VLAN 2.

```
[DeviceE] interface bridge-aggregation 3
[DeviceE-Bridge-Aggregation3] port link-type trunk
[DeviceE-Bridge-Aggregation3] port trunk permit vlan 2
[DeviceE-Bridge-Aggregation3] quit
```

Create VLAN-interface 2 and assign it an IP address.

```
[DeviceE] interface vlan-interface 2
[DeviceE-vlan-interface2] ip address 10.1.1.100 24
[DeviceE-vlan-interface2] quit
```

7. Configure Device F:

Create Layer 2 aggregate interface Bridge-Aggregation 5 and configure the interface to operate in dynamic mode.

```
<DeviceF> system-view
[DeviceF] interface bridge-aggregation 5
[DeviceF-Bridge-Aggregation5] link-aggregation mode dynamic
[DeviceF-Bridge-Aggregation5] quit
```

Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 5.

```
[DeviceF] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceF-if-range] port link-aggregation group 5
[DeviceF-if-range] quit
```

Create VLAN 3.

```
[DeviceF] vlan 3
[DeviceF-vlan3] quit
```

Set the link type of Bridge-Aggregation 5 to trunk, and assign it to VLAN 3.

```
[DeviceF] interface bridge-aggregation 5
[DeviceF-Bridge-Aggregation5] port link-type trunk
[DeviceF-Bridge-Aggregation5] port trunk permit vlan 3
[DeviceF-Bridge-Aggregation5] quit
```

Create VLAN-interface 3 and assign it an IP address.

```
[DeviceF] interface vlan-interface 3
[DeviceF-vlan-interface3] ip address 20.1.1.100 24
[DeviceF-vlan-interface3] quit
```

Using GIR to upgrade or replace DR member devices

Upgrading the secondary device (Device B)

1. Configure the maintenance mode and switch traffic to the primary device:

Configure the secondary device (Device B) to enter maintenance mode. Related route and aggregation settings will be automatically isolated to switch traffic to the primary device (Device A).

```
<DeviceB> system-view
```

```
[DeviceB] gir system-mode maintenance
Collecting commands... Please wait.
Configuration to be applied:
   bgp 200
     isolate enable
   isis 1
     isolate enable
   ospf 1 router-id 11.11.11.11
     isolate enable
   sleep instance 1 interval 30
   link-aggregation lacp isolate
Do you want to continue? [Y/N]: y
Generated a snapshot: before_maintenance.
Applying: bgp 200
Applying: isolate enable
Applying: isis 1
Applying: isolate enable
Applying: ospf 1 router-id 11.11.11.11
Applying: isolate enable
Applying: sleep instance 1 interval 30
Applying: link-aggregation lacp isolate
Waiting 120 seconds to release the CLI.
Changed to maintenance mode successfully.
```

Save the configuration. If you do not save the configuration, the device will be in normal mode after a successful upgrade and restart, which might result in traffic loss during switchback.

```
[DeviceB] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The startup.cfg file already exists.
Compared with the startup.cfg file, The current configuration adds 6 commands and
deletes 0 commands.
If you want to see the configuration differences, please cancel this operation, and
then use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Configuration is saved to device successfully.
[DeviceB] quit
```

2. Specify the upgrade file and reboot the device

Specify the next startup image file.

```
<DeviceB> boot-loader file flash:/s9850_6850-f6633.ipe all main
```

(Optional.) Specify the next startup configuration file.

```
<DeviceB> startup saved-configuration flash:/drni_new.cfg
```

Identify whether the device will use the newly loaded image file and configuration file for the next startup.

```
<DeviceB> display boot-loader
Software images on slot 1:
```

```
Current software images:
  flash:/s9850_6850-cmw710-boot-f6632.bin
  flash:/s9850_6850-cmw710-system-f6632.bin
Main startup software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Backup startup software images:
  None
<DeviceB> display startup
MainBoard:
 Current startup saved-configuration file: flash:/drni_old.cfg
 Next main startup saved-configuration file: flash:/drni_new.cfg
 Next backup startup saved-configuration file: NULL
```

Reboot the device.

```
<DeviceB> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[flash:/drni_old.cfg]
(To leave the existing filename unchanged, press the enter key):startup.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
```

3. Identify whether the DRNI upgrade method is successful in maintenance mode:

Identify whether the image file has been upgraded to the target file and whether the configuration file is the target one.

```
<DeviceB> display boot-loader
Software images on slot 1:
Current software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Main startup software images:
  flash:/s9850_6850-cmw710-boot-f6633.bin
  flash:/s9850_6850-cmw710-system-f6633.bin
Backup startup software images:
  None
<DeviceB> display startup
MainBoard:
 Current startup saved-configuration file: flash:/drni_new.cfg
 Next main startup saved-configuration file: flash: /drni_new.cfg
 Next backup startup saved-configuration file: NULL
```

Identify whether the device is operating normally.

```
<DeviceB> display device
Slot Type               State    Subslot  Soft Ver                    Patch Ver
1    S6850-56HF         Master   0        S6850-56HF-6633             None
```

Identify whether the configuration is restored.

After startup, execute the **display current-configuration** command in any view to see the current configuration of the device. Execute the **display diff current-configuration configfile flash:/XXX.cfg** command in any view to compare the running configuration file with the one saved in the storage device and check for any lost or changed configurations.

Display the DRNI state. The **IPP state** field should be **UP** when the device is operating normally.

```
<DeviceB> display drni summary
Flags: A -- Aggregate interface down, B -- No peer DR interface configured
       C -- Configuration consistency check failed

IPP: BAGG2
IPP state (cause): UP
Keepalive link state (cause): UP

                    DR interface information
DR interface  DR group  Local state (cause)  Peer state  Remaining down time(s)
BAGG3         3         DOWN (A)             UP          -
```

4. Switch the traffic back to the secondary device:

Switch the device back to normal mode and switch the traffic to the secondary device.

```
[DeviceB] undo gir system-mode maintenance
Collecting commands... Please wait.
Configuration to be applied:
   undo link-aggregation lacp isolate
   sleep instance 1 interval 30
   ospf 1 router-id 11.11.11.11
     undo isolate enable
   isis 1
     undo isolate enable
   bgp 200
     undo isolate enable
Do you want to continue? [Y/N]: y
Applying: undo link-aggregation lacp isolate
Applying: sleep instance 1 interval 30
Applying: ospf 1 router-id 11.11.11.11
Applying: undo isolate enable
Applying: isis 1
Applying: undo isolate enable
Applying: bgp 200
Applying: undo isolate enable
Waiting 120 seconds to generate a snapshot.
Generated a snapshot: after_maintenance.
Changed to normal mode successfully.
```

5. After traffic switchback completes, identify whether the service is operating normally:

You can identify whether the service is operating normally in either of the following methods:

- Compare the collected entries (such as the routing table, FIB table, and MAC address table entries) with those before the upgrade to check for any losses. Compare the service traffic before and after the upgrade to ensure consistency.

- Together with maintenance staff, identify whether service is operating properly and servers are operating normally.

6. Identify whether the device is in normal mode.
7. Save the configuration. The secondary device upgrade is complete.

Upgrading the primary device (Device A)

Upgrade Device A following the steps in "Upgrading the secondary device (Device B)." (Details not shown.)

Upgrading the secondary device (Device D)

Upgrade Device D following the steps in "Upgrading the secondary device (Device B)." (Details not shown.)

Upgrading the primary device (Device C)

Upgrade Device C following the steps in "Upgrading the secondary device (Device B)." (Details not shown.)

Replacing a faulty M-LAG member device

If you need a shorter convergence time and the faulty device can be switched to maintenance mode for replacement, follow these steps to replace it:

1. Execute the **gir system-mode maintenance** command on the faulty device to switch the device from normal mode to maintenance mode and save the configuration.
2. Import the fault device's configuration file to the new device.
3. Specify the image file and configuration file on the new device, and then reboot the device to apply the image file and configuration file.
4. Power off the new device or shut down all physical interfaces.
5. Shut down all physical interfaces on the faulty device or power off the faulty device. (When replacing multiple devices, power off the devices as a best practice.)
6. Replace the faulty device.
7. Connect the cables to the new device.
8. Power on the new device or bring up all physical interfaces.
9. Execute the **undo gir system-mode maintenance** command on the new device to switch from maintenance mode to normal mode and save the configuration.

Verifying the configuration

Verifying the configuration

1. Take Device A as an example to verify the DR system configuration.

   # Display information about tunnel interfaces on Device A. The output shows that the tunnel interface in VXLAN mode is up and the tunnel source IP is 1.1.1.1.

```
<DeviceA> display interface Tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1464
Internet protocol processing: Disabled
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
```

```
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Tunnel source 1.1.1.1, destination 2.2.2.2
Tunnel protocol/transport UDP_VXLAN/IP
Last 300 seconds input rate: 1 bytes/sec, 8 bits/sec, 0 packets/sec
Last 300 seconds output rate: 80 bytes/sec, 640 bits/sec, 0 packets/sec
Input: 26 packets, 1974 bytes, 0 drops
Output: 340 packets, 29514 bytes, 0 drops
```

Display the VSI information on Device A. The output shows that an AC is automatically created on the IPL and associated with a VSI.

```
<DeviceA> display l2vpn vsi verbose
VSI Name: vpna
  VSI Index               : 0
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
  Gateway Interface       : VSI-interface 1
  VXLAN ID                : 10
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel1              0x5000001  UP       Manual      Disabled
  ACs:
    AC                                Link ID    State       Type
    BAGG3 srv1000                     0          Up          Manual
    BAGG2 srv2                        1          Up          Dynamic (M-LAG)

VSI Name: vpnb
  VSI Index               : 1
  VSI State               : Up
  MTU                     : 1500
  Bandwidth               : -
  Broadcast Restrain      : -
  Multicast Restrain      : -
  Unknown Unicast Restrain: -
  MAC Learning            : Enabled
  MAC Table Limit         : -
  MAC Learning rate       : -
  Drop Unknown            : -
  Flooding                : Enabled
  Statistics              : Disabled
```

```
  Gateway Interface       : VSI-interface 2
  VXLAN ID                : 20
  Tunnels:
    Tunnel Name          Link ID    State    Type        Flood proxy
    Tunnel1              0x5000001  UP       Manual      Disabled
```

2. Verify that hosts can access each other.

   VMs Device E and Device F can access each other. If the link between Device E and either Device A or Device B disconnects, Device E and Device F can still communicate through another device.

3. Verify packet loss during an upgrade.

   During the upgrade of Device A, monitor the packet loss in traffic between Device G and Device E. Empirical data shows no packet loss occurs between them.

Configuration files

- Device A:

```
#
vlan 1

#
vlan 2

#
vlan 11

#
 l2vpn enable

#
vsi vpna
 gateway vsi-interface 1
 vxlan 10
  tunnel 1

#
vsi vpnb
 gateway vsi-interface 2
 vxlan 20
  tunnel 1

#
interface Bridge-Aggregation2
 port link-type trunk
 port trunk permit vlan all
 link-aggregation mode dynamic
 port m-lag peer-link 1

#
```

```
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic
 port m-lag group 3

#
 service-instance 1000
  encapsulation s-vid 2
  xconnect vsi vpna

#
interface Bridge-Aggregation4

#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255

#
interface Vlan-interface2

#
interface Vlan-interface11
 ip address 11.1.1.1 255.255.255.0

#
interface GigabitEthernet1/0/4
 port link-mode route
 combo enable copper
 ip address 60.1.1.1 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 11
 combo enable copper

#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
 port link-aggregation group 3

#
interface HundredGigE1/0/2
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2

#
interface HundredGigE1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 2

#
interface Vsi-interface1
 ip address 10.1.1.1 255.255.255.0
 mac-address 0001-0001-0001
 local-proxy-arp enable
 distributed-gateway local

#
interface Vsi-interface2
 ip address 20.1.1.1 255.255.255.0
 mac-address 0002-0002-0002
 local-proxy-arp enable
 distributed-gateway local

#
interface Tunnel1 mode vxlan
 source 1.1.1.1
 destination 2.2.2.2

#
 m-lag restore-delay 180
 m-lag system-mac 0001-0001-0001
 m-lag system-number 1
 m-lag system-priority 10
 m-lag keepalive ip destination 60.1.1.2 source 60.1.1.1
 m-lag mad exclude interface GigabitEthernet0/0/2
 m-lag mad exclude interface LoopBack0
 m-lag mad exclude interface Vlan-interface11
 m-lag mad exclude interface Vsi-interface1
 m-lag mad exclude interface Vsi-interface2

#
 arp distributed-gateway dynamic-entry synchronize
```

- Device B (Details not shown)
- Device C (Details not shown)
- Device D (Details not shown)
- Device E:

```
#
vlan 1

#
vlan 2

#
interface Bridge-Aggregation3
 port link-type trunk
 port trunk permit vlan 1 to 2
 link-aggregation mode dynamic

#
interface Vlan-interface2
 ip address 10.1.1.100 255.255.255.0

#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
 port link-aggregation group 3

#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2
 combo enable copper
 port link-aggregation group 3
```

- Device F (Details not shown)