H3C Devices CLI Reference

Contents

Comware 7 CLI views 1

Introduction 1
Entering a view 2
Exiting a view 2
Entering user view 2
Entering system view 2
Entering a feature view 3
Related documentation 3

Using the CLI 4

Introduction 4
Accessing the CLI online help 4
Using the undo form of a command 5
Entering a command 5
Editing a command line 5
Entering a text or string type value for an argument 6
Entering an interface type 6
Abbreviating commands 7
Configuring and using command aliases 8
Configuring and using hotkeys 9
Enabling redisplaying entered-but-not-submitted commands 10
Understanding command-line syntax error messages 11
Using the command history feature 11
About command history buffers 11
Command buffering rules 12
Managing and using the command history buffers 12
Repeating commands in the command history buffer for a user line 12
Controlling the CLI output 13
Pausing between screens of output 13
Numbering each output line from a display command 14
Filtering the output from a display command 14
Saving the output from a display command to a file 17
Viewing and managing the output from a display command effectively 18
Related documentation 19

Comware 7 CLI views

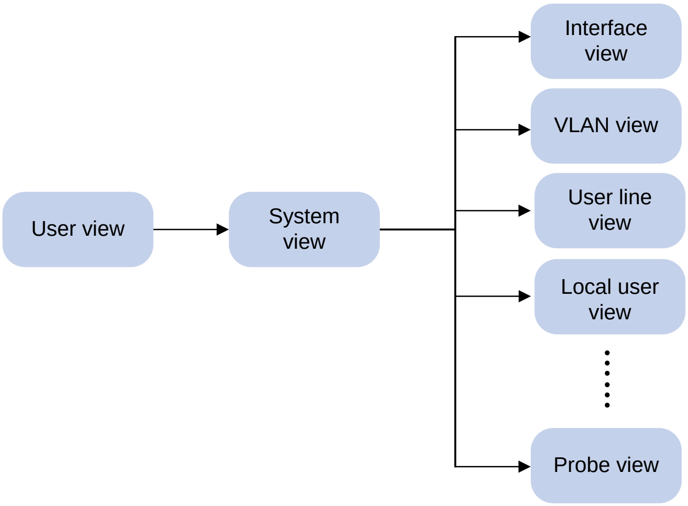
Introduction

The following information describes CLI views provided by Comware 7.

Commands are grouped in different views by feature. To use a command, you must enter its view.

CLI views are hierarchically organized, as shown in Figure 1. Each view has a unique prompt, from which you can identify where you are and what you can do. For example, the prompt `[Sysname-vlan100]` shows that you are in VLAN 100 view and can configure attributes for that VLAN.

Figure 1 CLI views



You are placed in user view immediately after you log in to the CLI.

In user view, you can perform the following tasks:

- Perform basic operations including display, debug, file management, FTP, Telnet, clock setting, and reboot.
- Enter system view.

In system view, you can perform the following tasks:

- Configure settings that affect the device as a whole, such as the daylight saving time, banners, and hotkeys.
- Enter feature views.

  For example, you can perform the following tasks:

  - Enter interface view to configure interface parameters.
  - Enter VLAN view to add ports to the VLAN.
  - Enter user line view to configure login user attributes.

  A feature view might have child views. For example, NQA operation view has the child view HTTP operation view.

To display all commands available in a view, enter a question mark (?) at the view prompt.

Entering a view

Enter different views as follows:

- You are placed in user view immediately after you log in to the CLI.
- To enter system view, use the **system-view** command in user view.
- To enter a feature view from system view, use the corresponding command. A feature view might have child views.

Exiting a view

Use one of the following methods to exit a view except user view, Tcl configuration view, Python shell view, public key code view, and public key view:

- Use the **quit** command to return to the upper-level view from a view.
- Use the **return** command to return to user view.
- Press **Ctrl+Z** to return to user view.

Using the **quit** command in user view terminates your connection to the device. The **return** command is not supported in user view.

To exit Tcl configuration view, Python shell view, public key code view, and public key view, use the following methods:

- To return to user view from Tcl configuration view, use the **tclquit** command.
- To return to user view from Python shell view, use the **exit()** command.
- To return to the upper-level view (public key view) from public key code view, use **public-key-code end** the command.
- To return to system view from public key view, use the **peer-public-key end** command.

Entering user view

You are placed in user view immediately after you log in to the CLI.

In user view, you can perform the following tasks:

- Perform basic operations including display, debug, file management, FTP, Telnet, clock setting, and reboot.
- Enter system view.

The prompt for user view is <*system name*>, for example, <Sysname>. You can configure the system name as needed.

Entering system view

To enter system view, use the **system-view** command in user view as follows:

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

In system view, you can configure settings that affect the device as a whole, such as the daylight saving time, banners, and hotkeys.

Entering a feature view

You can enter features from system view. For example:

- Enter Ethernet interface view as follows:
  ```
  <Sysname> system-view
  [Sysname] interface GigabitEthernet 1/0/1
  [Sysname-GigabitEthernet1/0/1]
  ```
- Enter VLAN view as follows:
  ```
  <Sysname> system-view
  [Sysname] vlan 2
  [Sysname-vlan2]
  ```

Related documentation

- CLI configuration in the fundamentals configuration guide for the device
- CLI commands in the fundamentals command reference for the device

Using the CLI

Introduction

The following information describes how to use the CLI.

Accessing the CLI online help

The CLI online help is context sensitive. Enter a question mark at any prompt or in any position of a command to display all available options.

To access the CLI online help, use one of the following methods:

- Enter a question mark at a view prompt to display the first keyword of every command available in the view. For example:

```
<Sysname> ?
User view commands:
  archive             Archive configuration
  arp                 Address Resolution Protocol (ARP) module
  backup              Backup the startup configuration file to a TFTP server
  boot-loader         Software image file management
...
```

- Enter a space and a question mark after a command keyword to display all available keywords and arguments.
  - If the question mark is in the place of a keyword, the CLI displays all possible keywords, each with a brief description. For example:

```
<Sysname> terminal ?
  debugging  Enable to display debugging logs on the current terminal
  logging    Display logs on the current terminal
  monitor    Enable to display logs on the current terminal
```

  - If the question mark is in the place of an argument, the CLI displays the description for the argument. For example:

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
  <1-4094>  Vlan-interface interface number
[Sysname] interface vlan-interface 1 ?
  <cr>
[Sysname] interface vlan-interface 1
```

  <1-4094> is the value range for the argument. **<cr>** indicates that the command is complete and you can press **Enter** to use the command.

- Enter an incomplete keyword string followed by a question mark to display all keywords starting with that string. The CLI also displays the descriptions for the keywords. For example:

```
<Sysname> f?
  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
```

```
<Sysname> display ftp?
  ftp          FTP module
  ftp-server   FTP server information
  ftp-user     FTP user information
```

Using the undo form of a command

Most configuration commands have an **undo** form for the following tasks:

- Canceling a configuration.
- Restoring the default.
- Disabling a feature.

For example, the **`info-center enable`** command enables the information center. The **`undo info-center enable`** command disables the information center.

Entering a command

When you enter a command, you can perform the following tasks:

- Use keys or hotkeys to edit the command line.
- Use abbreviated keywords or keyword aliases.

Editing a command line

To edit a command line, use the keys listed in Table 1 or the hotkeys listed in Table 4. When you are finished, you can press **Enter** to execute the command.

The command edit buffer can contain a maximum of 511 characters. If the total length of a command line exceeds the limit after you press **Tab** to complete the last keyword or argument, the system does not complete the keyword.

Table 1 Command line editing keys

Keys	Function
Common keys	If the edit buffer is not full, pressing a common key inserts a character at the cursor and moves the cursor to the right. The edit buffer can store up to 511 characters. Unless the buffer is full, all common characters that you enter before pressing **Enter** are saved in the edit buffer.
Backspace	Deletes the character to the left of the cursor and moves the cursor back one character.
Left arrow key (←)	Moves the cursor one character to the left.
Right arrow key (→)	Moves the cursor one character to the right.
Up arrow key (↑)	Displays the previous command in the command history buffer.
Down arrow key (↓)	Displays the next command in the command history buffer.
Tab	If you press **Tab** after typing part of a keyword, the system automatically completes the keyword. • If a unique match is found, the system displays the complete keyword. • If there is more than one match, press **Tab** multiple times to pick the keyword you want to enter. • If there is no match, the system does not modify what you entered but displays it again in the next line.

The device supports the following special commands:

- #—Used by the system in a configuration file as separators for adjacent sections.
- **version**—Used by the system in a configuration file to indicate the software version information. For example, **version 7.1. xxx**, **Release xxx**.

These commands are special because of the following reasons:

- These commands are not intended for you to use at the CLI.
- You can enter the **#** command in any view or the **version** command in system view, or enter any values for them. For example, you can enter **# abc** or **version abc**. However, the settings do not take effect.
- The device does not provide any online help information for these commands.

Entering a text or string type value for an argument

A text type argument value can contain any characters except question marks (?).

A string type argument value can contain any printable characters except question marks (?).

- To include a quotation mark (") or backward slash (\) in a string type argument value, prefix the character with an escape key (\), for example, \" and \\.
- To include a blank space in a string type argument value, enclose the value in quotation marks, for example, "my device".

A specific argument might have more requirements. For more information, see the relevant command reference.

To enter a printable character, you can enter the character or its ASCII code in the range of 32 to 126.

Entering an interface type

You can enter an interface type in one of the following formats:

- Full spelling of the interface type.
- An abbreviation that uniquely identifies the interface type.
- Acronym of the interface type.

For a command line, all interface types are case insensitive. Table 2 shows the full spellings and acronyms of interface types.

For example, to use the **interface** command to enter the view of interface GigabitEthernet 1/0/1, you can enter the command line in the following formats:

- **interface gigabitethernet 1/0/1**
- **interface g 1/0/1**
- **interface ge 1/0/1**

Spaces between the interface types and interfaces are not required.

Table 2 Full spellings and acronyms of interface types

Full spelling	Acronym
Bridge-Aggregation	BAGG
Ethernet	Eth
EVI-Link	EVI
FiftyGigE	50GE

FortyGigE	FGE
FourHundredGigE	400GE
GigabitEthernet	GE
HundredGigE	HGE
InLoopBack	InLoop
LoopBack	Loop
M-Ethernet	ME
M-GigabitEthernet	MGE
Multicast Tunnel	MTunnel
NULL	NULL
Pex	PEX
RPR-Bridge	RPR-B
RPR-Router	RPR-R
Register-Tunnel	REG
Route-Aggregation	RAGG
SAN-Aggregation	SAGG
S-Channel	S-Ch
Schannel-Aggregation	SCH-AGG
Schannel-Bundle	SCH-B
Smartrate-Ethernet	SGE
Ten-GigabitEthernet	XGE
Tunnel	Tun
Tunnel-Bundle	Tunnel-B
TwentyGigE	TGE
Twenty-FiveGigE	WGE
Vfc	Vfc
Vsi-interface	Vsi
Vlan-interface	Vlan-int

Abbreviating commands

You can enter a command line quickly by entering incomplete keywords that uniquely identify the complete command. In user view, for example, commands starting with an **s** include **startup saved-configuration** and **system-view**. To enter the **system-view** command, you need to type only **sy**. To enter the **startup saved-configuration** command, type **st s**.

You can also press **Tab** to complete an incomplete keyword.

Configuring and using command aliases

About this task

You can configure one or more aliases for a command or the starting keywords of commands. Then, you can use the aliases to execute the command or commands. If the command or commands have **undo** forms, you can also use the aliases to execute the **undo** command or commands.

For example, if you configure the **shiprt** alias for **display ip routing-table**, you can enter **shiprt** to execute the **display ip routing-table** command. If you configure the **ship** alias for **display ip**, you can use **ship** to execute all commands starting with **display ip**, including:

- Enter **ship routing-table** to execute the **display ip routing-table** command.
- Enter **ship interface** to execute the **display ip interface** command.

The device provides a set of system-defined command aliases, as listed in Table 3.

Table 3 System-defined command aliases

Command alias	Command or command keyword
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

Restrictions and guidelines

A command alias can be used only as the first keyword of a command or the second keyword of the **undo** form of a command.

After you successfully execute a command by using an alias, the system saves the command, instead of the alias, to the running configuration.

The command string can include up to nine parameters. Each parameter starts with the dollar sign ($) and a sequence number in the range of 1 to 9. For example, you can configure the alias **shinc** for the **display ip $1 | include $2** command. Then, to execute the **display ip routing-table | include Static** command, you need to enter only **shinc routing-table Static**.

To use an alias for a command that has parameters, you must specify a value for each parameter. If you fail to do so, the system informs you that the command is incomplete and displays the command string represented by the alias.

System-defined command aliases cannot be deleted.

Procedure

1. Enter system view.

   system-view

2. Configure a command alias.

   alias *alias command*

   By default, the device has a set of command aliases, as listed in Table 3.

3. (Optional.) Display command aliases.

   display alias [*alias*]

   This command is available in any view.

Configuring and using hotkeys

About this task

The device supports a set of hotkeys. Pressing a hotkey executes the command or function assigned to the hotkey. Table 4 shows the hotkeys and their default definitions. You can configure all the hotkeys except **Ctrl+]**.

If a hotkey is also defined by the terminal software you are using to interact with the device, you can reconfigure the hotkey or remove the hotkey.

Restrictions and guidelines

A hotkey can correspond to only one command or function. If you assign multiple commands or functions to the same hotkey, the most recently assigned command or function takes effect.

A command or function can be assigned to multiple hotkeys. You can use any of the hotkeys to execute the command or function.

If a hotkey is also defined by the terminal software you are using to interact with the device, the terminal software definition takes effect.

Procedure

1. Enter system view.

   system-view

2. Assign a command to a hotkey.

   hotkey *hotkey* { *command* | **function** *function* | **none** }

   Table 4 shows the default definitions for the hotkeys.

3. (Optional.) Display hotkeys.

   display hotkey

   This command is available in any view.

Table 4 Default definitions for hotkeys

Hotkey	Function or command
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line**: Moves the cursor to the beginning of a line.
Ctrl+B	**move_the_cursor_one_character_to_the_left**: Moves the cursor one character to the left.
Ctrl+C	**stop_the_current_command**: Stops the current command.
Ctrl+D	**erase_the_character_at_the_cursor**: Deletes the character at the cursor.
Ctrl+E	**move_the_cursor_to_the_end_of_the_line**: Moves the cursor to the end of a line.
Ctrl+F	**move_the_cursor_one_character_to_the_right**: Moves the cursor one character to the right.
Ctrl+G	**display current-configuration**: Displays the running configuration.
Ctrl+H	**erase_the_character_to_the_left_of_the_cursor**: Deletes the character to the left of the cursor.
Ctrl+L	**display ip routing-table**: Displays the IPv4 routing table information.

Hotkey	Function or command
Ctrl+N	**display_the_next_command_in_the_history_buffer**: Displays the next command in the history buffer. Password configuration commands, if any, are skipped.
Ctrl+O	**undo debugging all**: Disables all debugging functions.
Ctrl+P	**display_the_previous_command_in_the_history_buffer**: Displays the previous command in the history buffer. Password configuration commands, if any, are skipped.
Ctrl+R	**redisplay_the_current_line**: Redisplays the current line.
Ctrl+T	N/A
Ctrl+U	N/A
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor**: Deletes the word to the left of the cursor.
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor**: Deletes all characters to the left of the cursor.
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line**: Deletes all characters from the cursor to the end of the line.
Ctrl+Z	**return_to_the_User_View**: Returns to user view.
Ctrl+]	**kill_incoming_connection_or_redirect_connection**: Terminates the current connection.
Esc+B	**move_the_cursor_back_one_word**: Moves the cursor back one word.
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word**: Deletes all characters from the cursor to the end of the word.
Esc+F	**move_the_cursor_forward_one_word**: Moves the cursor forward one word.

Enabling redisplaying entered-but-not-submitted commands

About this task

Your input might be interrupted by system information output. If redisplaying entered-but-not-submitted commands is enabled, the system redisplays your input after finishing the output. You can then continue entering the command line.

Procedure

1. Enter system view.

   ```
   system-view
   ```

2. Enable redisplaying entered-but-not-submitted commands.

   ```
   info-center synchronous
   ```

   By default, the system does not redisplay entered-but-not-submitted commands.

   For more information about this command, see information center commands in the network management and monitoring command reference for the device.

Understanding command-line syntax error messages

After you press **Enter** to submit a command, the command line interpreter examines the command syntax.

- If the command passes syntax check, the CLI executes the command.
- If the command fails syntax check, the CLI displays an error message.

Table 5 Common command-line syntax error messages

Syntax error message	Cause
% Unrecognized command found at '^' position.	The keyword in the marked position is invalid.
% Incomplete command found at '^' position.	One or more required keywords or arguments are missing.
% Ambiguous command found at '^' position.	The entered character sequence matches more than one command.
% Too many parameters found at '^' position.	The entered character sequence contains excessive keywords or arguments.
% Wrong parameter found at '^' position.	The argument in the marked position is invalid.

Using the command history feature

About command history buffers

The system automatically saves commands successfully executed by a login user to the following two command history buffers:

- Command history buffer for the user line.
- Command history buffer for all user lines.

Table 6 Comparison between the two types of command history buffers

Item	Command history buffer for a user line	Command history buffer for all user lines
Which commands are saved in the buffer?	Commands successfully executed by the current user of the user line.	Commands successfully executed by all login users.
Can commands in the buffer be displayed?	Yes.	Yes.
Can commands in the buffer be recalled?	Yes.	No.
Are buffered commands cleared when the user logs out?	Yes.	No.
Is the buffer size adjustable?	Yes.	No. The buffer size is fixed at 1024.

Command buffering rules

The system follows these rules when buffering commands:

- If you use incomplete keywords when entering a command, the system buffers the command in the exact form that you used.
- If you use an alias when entering a command, the system transforms the alias to the represented command or command keywords before buffering the command.
- If you enter a command in the same format multiple times in succession, the system buffers the command only once. If you enter a command in different formats multiple times, the system buffers each command format. For example, **`display cu`** and **`display current-configuration`** are buffered as two entries but successive repetitions of **`display cu`** create only one entry.
- To buffer a new command when a buffer is full, the system deletes the oldest command entry in the buffer.

Managing and using the command history buffers

Displaying the commands in command history buffers

To display the commands in command history buffers, execute the following commands in any view:

- Display the commands in command history buffers for a user line.

  ```
  display history-command
  ```
- Display the commands in command history buffers for all user lines.

  ```
  display history-command all
  ```

Recalling commands in the command history buffer for a user line

IMPORTANT:

Password configuration commands cannot be recalled.

Use up and down arrow keys to navigate to a command and press **Enter**.

Setting the size of the command history buffer for a user line

Use the **`history-command max-size`** command in user line or user line class view. For more information, see login management commands in the fundamentals command reference for the device.

Repeating commands in the command history buffer for a user line

About this task

You can recall and execute commands in the command history buffer for the current user line multiple times.

Restrictions and guidelines

The **`repeat`** command is available in any view. However, to repeat a command, you must first enter the view for the command. To repeat multiple commands, you must first enter the view for the first command.

The **`repeat`** command executes commands in the order they were executed.

The system starts a timer and waits for your interaction when it repeats an interactive command. If you do not provide the required information at prompt before the timer expires, the system skips the interactive command.

The system skips all password configuration commands.

Procedure

To repeat commands in the command history buffer for the current user line, execute the following command:

```
repeat [ number ] [ count times ] [ delay seconds ]
```

Controlling the CLI output

This section describes the CLI output control features that help you identify the desired output.

Pausing between screens of output

About this task

The device can automatically pause after displaying a specific number of lines if the output is too long to fit on one screen. At a pause, the device displays **----more----**. You can use the keys described in Table 7 to display more information or stop the display.

You can also disable pausing between screens of output for the current session. Then, all output is displayed at one time and the screen is refreshed continuously until the final screen is displayed.

Table 7 Output controlling keys

Keys	Function
Space	Displays the next screen.
Enter	Displays the next line.
Ctrl+C	Stops the display and cancels the command execution.
<PageUp>	Displays the previous page.
<PageDown>	Displays the next page.

Disabling pausing between screens of output

To disable pausing between screens of output, execute the following command in user view:

```
screen-length disable
```

The default depends on the settings of the **screen-length** command in user line view. The following are the default settings for the **screen-length** command:

- Pausing between screens of output is enabled.
- The maximum number of lines to be displayed at a time is 24.

For more information about the **screen-length** command, see login management commands in the fundamentals command reference for the device.

This command is a one-time command and takes effect only for the current CLI session.

Numbering each output line from a display command

About this task

For easy identification, you can use the **| by-linenum** option to display a number for each output line from a **display** command.

Each line number is displayed as a 5-character string and might be followed by a colon (:) or hyphen (-). If you specify both **| by-linenum** and **| begin** *regular-expression* for a **display** command, a hyphen is displayed for all lines that do not match the regular expression.

Procedure

To number each output line from a **display** command, execute the following command in any view:

display *command* **| by-linenum**

Example

# Display information about VLAN 999, numbering each output line.

```
<Sysname> display vlan 999 | by-linenum
    1:  VLAN ID: 999
    2:  VLAN type: Static
    3:  Route interface: Configured
    4:  IPv4 address: 192.168.2.1
    5:  IPv4 subnet mask: 255.255.255.0
    6:  Description: For LAN Access
    7:  Name: VLAN 0999
    8:  Tagged ports:   None
    9:  Untagged ports: None
```

Filtering the output from a display command

About this task

You can use the [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128> option to filter the output from a **display** command.

- You can use the option to specify a maximum of 128 filter conditions. The system displays only output lines that meet all the conditions.
- **by-linenum**—Displays a number before each output line. You need to specify this keyword in only one filter condition.
- **begin**—Displays the first line matching the specified regular expression and all subsequent lines.
- **exclude**—Displays all lines not matching the specified regular expression.
- **include**—Displays all lines matching the specified regular expression.
- *regular-expression*—A case-sensitive string of 1 to 256 characters, which can contain the special characters described in Table 8.

Table 8 Special characters supported in a regular expression

Characters	Meaning	Examples
^	Matches the beginning of a line.	"^u" matches all lines beginning with "u". A line beginning with "Au" is not matched.
$	Matches the end of a line.	"u$" matches all lines ending with "u". A line ending with "uA" is not matched.

Characters	Meaning	Examples
. (period)	Matches any single character.	".s" matches "as" and "bs".
*	Matches the preceding character or string zero, one, or multiple times.	"zo*" matches "z" and "zoo", and "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or string one or multiple times.	"zo+" matches "zo" and "zoo", but not "z".
|	Matches the preceding or succeeding string.	"def|int" matches a line containing "def" or "int".
( )	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).	"(123A)" matches "123A". "408(12)+" matches "40812" and "408121212", but not "408".
\N	Matches the preceding strings in parentheses, with the *Nth* string repeated once.	"(string)\1" matches a string containing "stringstring". "(string1)(string2)\2" matches a string containing "string1string2string2". "(string1)(string2)\1\2" matches a string containing " string1string2string1string2".
[ ]	Matches a single character in the brackets.	"[16A]" matches a string containing 1, 6, or A; "[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, []abc]. There is no such limit on "[".
[^]	Matches a single character that is not in the brackets.	"[^16A]" matches a string that contains one or more characters except for 1, 6, or A, such as "abc". A match can also contain 1, 6, or A (such as "m16"), but it cannot contain these three characters only (such as 1, 16, or 16A).
{n}	Matches the preceding character *n* times. The number *n* must be a nonnegative integer.	"o{2}" matches "food", but not "Bob".
{n,}	Matches the preceding character *n* times or more. The number *n* must be a nonnegative integer.	"o{2,}" matches "foooood", but not "Bob".
{n,m}	Matches the preceding character *n* to *m* times or more. The numbers *n* and *m* must be nonnegative integers and *n* cannot be greater than *m*.	" o{1,3}" matches "fod", "food", and "foooood", but not "fd".
\<	Matches a string that starts with the pattern following \<. A string that contains the pattern is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches a string that ends with the pattern preceding \>. A string that contains the pattern is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\>" matches "undo" and "cdo".
\b	Matches a word that starts with the pattern following \b or ends with the pattern preceding \b.	"er\b" matches "never", but not "verb" or "erase". "\ber" matches "erase", but not "verb" or "never".

Characters	Meaning	Examples
\B	Matches a word that contains the pattern but does not start or end with the pattern.	"er\B" matches "verb", but not "never" or "erase".
\w	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"v\w" matches "vlan" and "service".
\W	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\Wa" matches "-a", but not "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	"\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "\b".

Restrictions and guidelines

The required filtering time increases with the complexity of the regular expression. To abort the filtering process, press **Ctrl+C**.

Examples

# Display the running configuration, starting from the first configuration line that contains **line**.

```
<Sysname> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
...
```

# Display brief information about interfaces in up state.

```
<Sysname> display interface brief | exclude DOWN
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)    --
NULL0                UP   UP(s)    --
Vlan1                UP   UP       192.168.1.83

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   1000M(a) F(a)   A    1
```

# Display SNMP-related running configuration lines.

```
<Sysname> display current-configuration | include snmp
snmp-agent
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname public
```

# Display log entries in the log buffer that contain both **SHELL** and **VTY**.

```
<Sysname> display logbuffer | include SHELL | include VTY
%Sep  6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Sep  6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

Saving the output from a display command to a file

About this task

A **display** command shows certain configuration and operation information of the device. Its output might vary over time or with user configuration or operation. You can save the output to a file for future retrieval or troubleshooting.

Use one of the following methods to save the output from a **display** command:

- Save the output to a separate file. Use this method if you want to use one file for a single **display** command.
- Append the output to the end of a file. Use this method if you want to use one file for multiple **display** commands.

Procedure

To save the output from a **display** command to a file, use one of the following commands in any view:

- Save the output from a **display** command to a separate file.

  display *command* **>** *filename*

- Append the output from a **display** command to the end of a file.

  display *command* **>>** *filename*

Examples

# Save the VLAN 1 settings to a separate file named **vlan.txt**.

```
<Sysname> display vlan 1 > vlan.txt
```

# Verify that the VLAN 1 settings are saved to the file **vlan.txt**.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
```

# Append the VLAN 999 settings to the end of the file **vlan.txt**.

```
<Sysname> display vlan 999 >> vlan.txt
```

# Verify that the VLAN 999 settings are appended to the end of the file **vlan.txt**.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IP address: 192.168.2.1
 Subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports: None
```

Viewing and managing the output from a display command effectively

You can use the following methods in combination to filter and manage the output from a **display** command:

- Numbering each output line from a display command
- Filtering the output from a display command
- Saving the output from a display command to a file

Procedure

To use multiple measures to view and manage the output from a **display** command effectively, execute the following command in any view:

display *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128> [**>** *filename* | **>>** *filename*]

Examples

# Save the running configuration to a separate file named **test.txt**, with each line numbered.

```
<Sysname> display current-configuration | by-linenum > test.txt
```

# Append lines including **snmp** in the running configuration to the file **test.txt**.

```
<Sysname> display current-configuration | include snmp >> test.txt
```

# Display the first line that begins with **user-group** in the running configuration and all the following lines.

```
<Sysname> display current-configuration | by-linenum begin user-group
```

```
114:  user-group system
115-  #
116-  return
```

// The colon (:) following a line number indicates that the line contains the string user-group. The hyphen (-) following a line number indicates that the line does not contain the string **user-group**.

Related documentation

- CLI configuration in the fundamentals configuration guide for the device.
- CLI commands in the fundamentals command reference for the device.

Login Management Quick Start Configuration Guide

Contents

Configuring console login 1

Introduction 1
Network configuration 1
Prerequisites 1
Procedure 3
Configuration files 6
Related documentation 6

Configuring Telnet login 7

Introduction 7
Network configuration 7
Prerequisites 7
Procedure 8
Verifying the configuration 8
Configuration files 9
Related documentation 9

Configuring console login with local authentication 10

Introduction 10
Prerequisites 10
Procedure 10
Verifying the configuration 11
Configuration files 11
Related documentation 12

Recovering the password of the console port 13

Introduction 13
Network configuration 13
Procedure 13
Configuration files 18
Related documentation 18

Recovering the password for Telnet/Web login 19

Introduction 19
Network configuration 19
Procedure 19
Configuration files 19
Related documentation 20

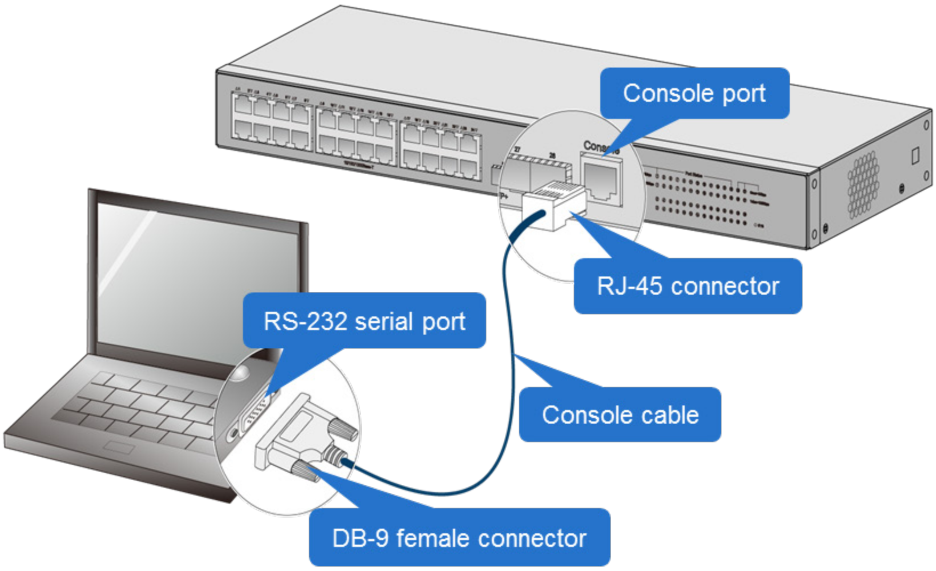
Configuring console login

Introduction

The following information uses an example to describe the basic procedure for logging in to the device through a console port.

Network configuration

Figure 1 Connecting to the console port on the device with a DB9-to-RJ45 console cable



Prerequisites

Before logging in to the device through a console port, make sure the following requirements are met:

- The terminal software PuTTY or VTP is installed.
- Make sure the console cable is supported by the device. Table 1 and Table 2 show the console cables supported by H3C devices. The available console cables vary by device model. For more information, see the installation guide for the device.

NOTE:

The pin definition for an RJ-45 connector of a serial console cable varies by device model. To avoid abnormal configuration terminal display, use a serial console cable provided by H3C, as shown in Table 2. If you use a third-party serial console cable, make sure the pin definition for an RJ-45 connector is as shown in Table 3.

Table 1 Connection methods and console cables

Connection method	Console cable type	Configuration terminal-side connector	Switch-side connector
Using the serial console cable for connection	DB9-to-RJ45 console cable	DB-9 female connector	RJ-45 connector
	USB-to-RJ45 console cable	USB connector	RJ-45 connector
Using the mini USB console cable for connection	Mini USB console cable	USB connector	USB mini-Type B connector
Using the micro USB console cable for connection	Micro USB console cable	USB connector	USB micro-Type B connector

Table 2 Pictures of console cables

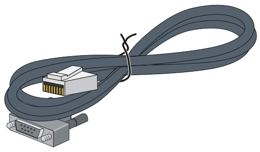
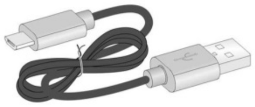
Console cable	Picture	Product code
DB9-to-RJ45 console cable		04042967
USB-to-RJ45 console cable		0404A1EE
Mini USB console cable		N/A
Micro USB console cable		N/A

Table 3 DB9-to-RJ45 console cable signal pinout

RJ-45	Signal	DB-9	Signal
1	RTS	8	CTS
2	DTR	6	DSR
3	TXD	2	RXD
4	SG	5	SG
5	SG	5	SG
6	RXD	3	TXD

7	DSR	4	DTR
8	CTS	7	RTS

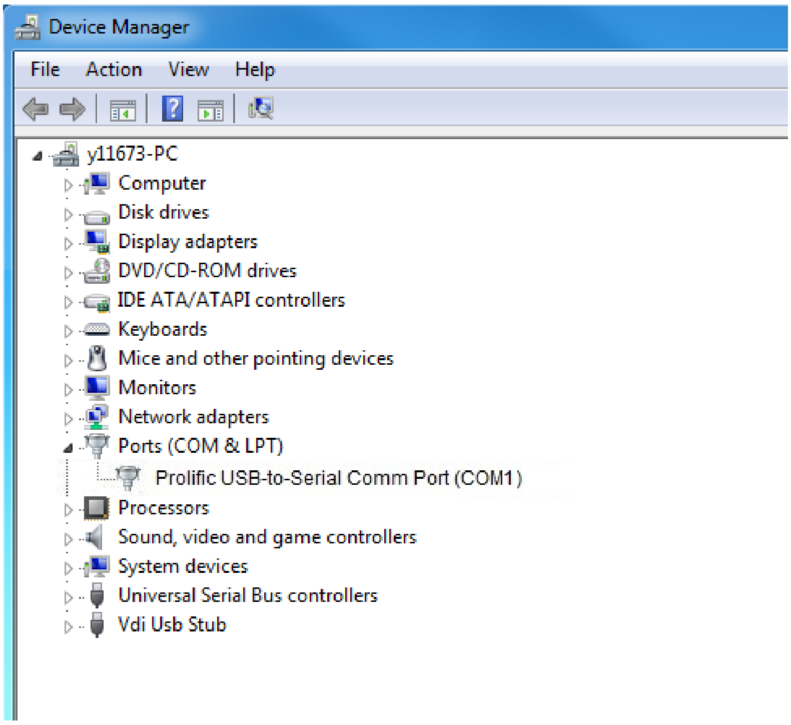
Procedure

1. As shown in Figure 1, use a DB9-to-RJ45 console cable to connect the PC to the device. Then, right-click Computer, and select Properties > Device Manager > Ports to identify communications ports used on the PC. This example uses port COM1, as shown in Figure 2.

IMPORTANT:

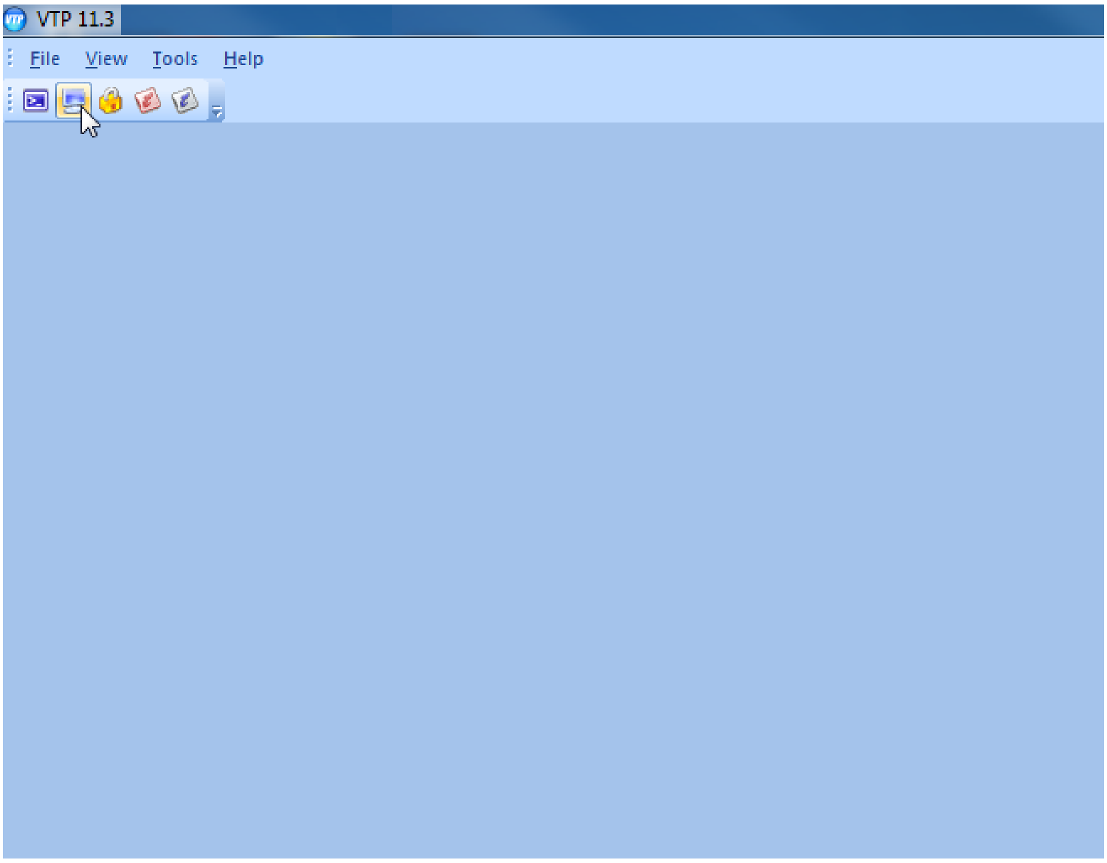
Before using a USB-to-RJ45 console cable, a mini USB console cable, or a micro USB console cable to connect the device to the PC, first download and install the corresponding driver on the PC for port identification. For more information about downloading and installing drivers, see the installation guide for the device.

Figure 2 Identifying the communications port



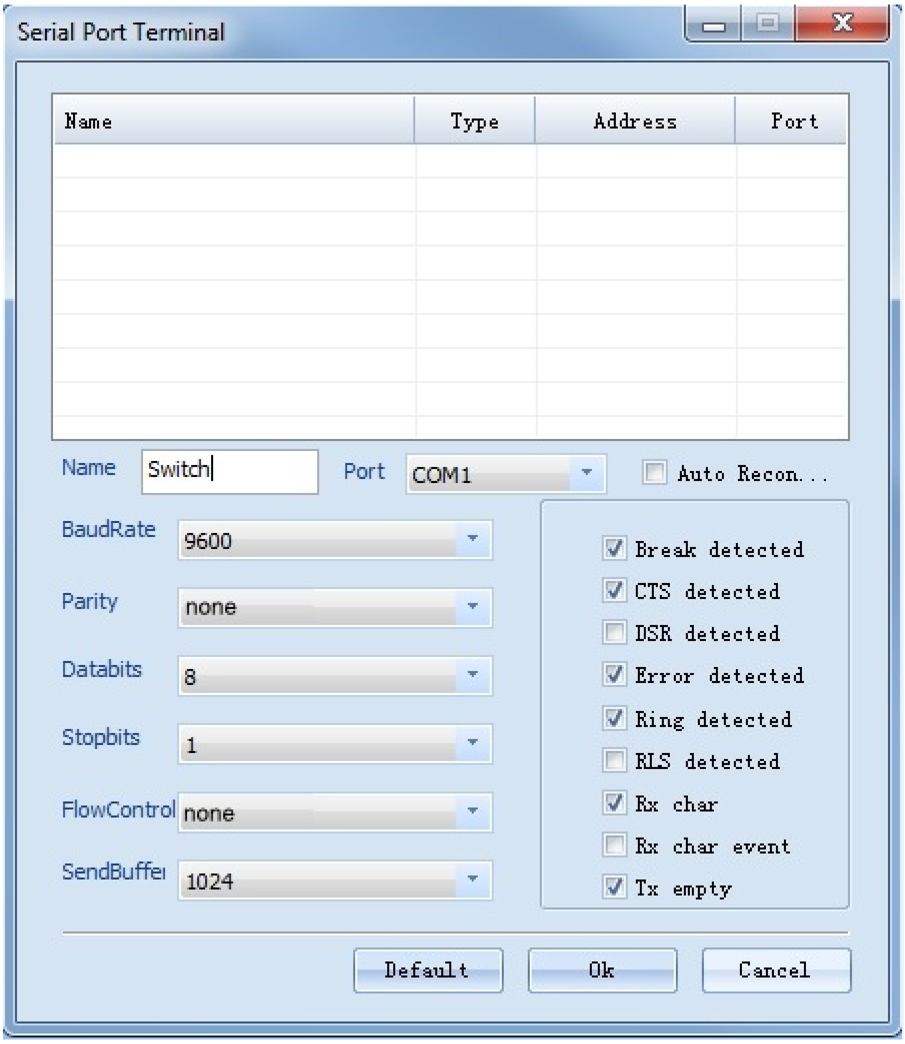
2. Open the terminal software on the PC to create a serial port terminal, as shown in Figure 3.

Figure 3 Creating a serial port terminal



3. As shown in Figure 4, enter device name Switch, select port COM1, configure the terminal parameters as follows, and then click **OK**:
   - **BaudRate**—9600 bps.
   - **Databits**—8.
   - **Stopbits**—1.
   - **Parity**—None.
   - **FlowControl**—None.

Figure 4 Configuring terminal parameters



Serial Port Terminal

Name	Type	Address	Port

Name: Switch

Port: COM1

☐ Auto Recon...

BaudRate: 9600

Parity: none

Databits: 8

Stopbits: 1

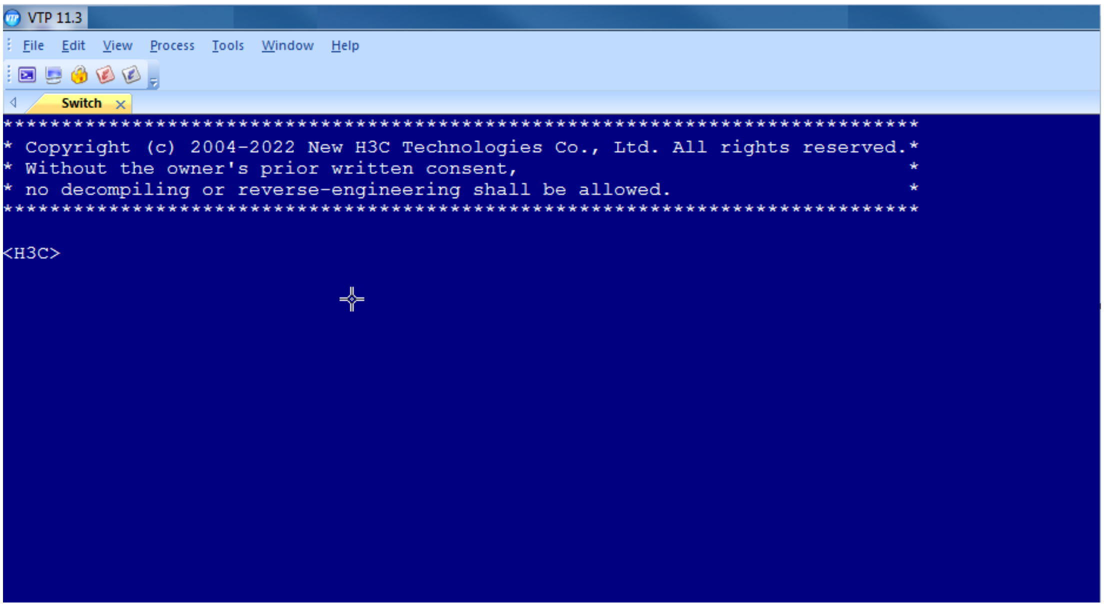
FlowControl: none

SendBuffer: 1024

☑ Break detected
☑ CTS detected
☐ DSR detected
☑ Error detected
☑ Ring detected
☐ RLS detected
☑ Rx char
☐ Rx char event
☑ Tx empty

4. Enter the system, as shown in Figure 5, which indicates that the PC is connected to the device by using the console cable successfully.

Figure 5 Connected to the device



```
******************************************************************************
* 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.                    *
******************************************************************************

<H3C>
```

Configuration files

None.

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.

Configuring Telnet login

Introduction

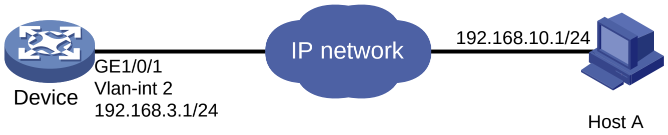
The following information uses an example to describe the basic Telnet login procedure.

Network configuration

As shown in Figure 6, 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.
- Assign the user role **network-admin** to the user.

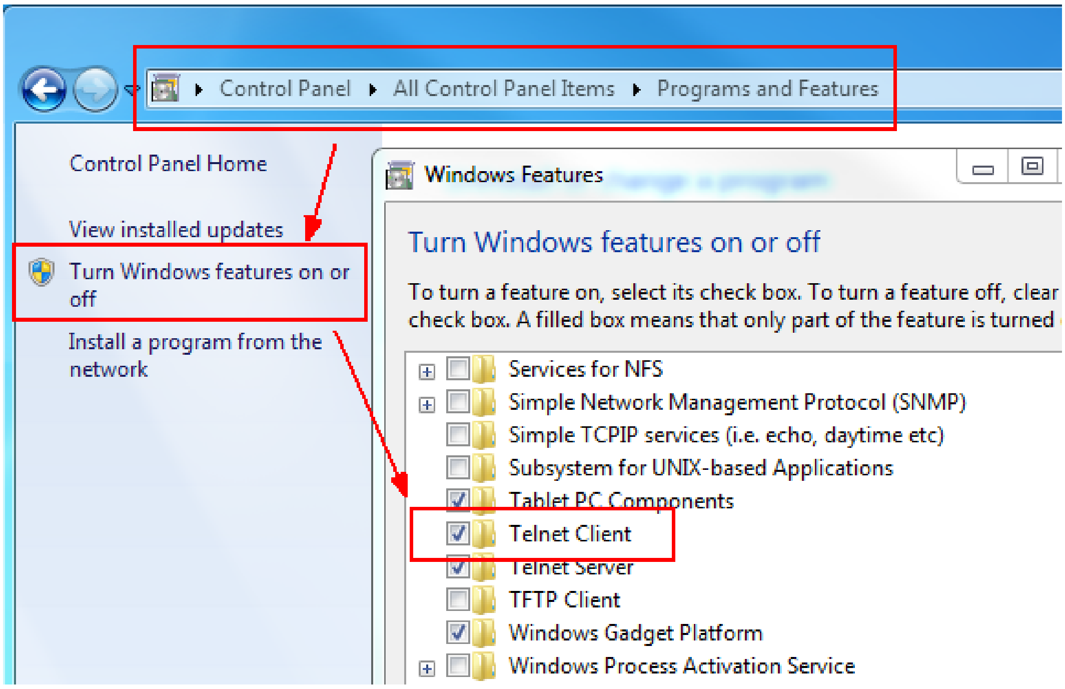
Figure 6 Network diagram



Prerequisites

- Configure an IP address for the device and obtain the IP address for the Telnet server. If the device and the Telnet server are not in the same subnet, make sure the device and the Telnet server can reach each other.
- The Command Prompt window of the Windows system can act as a Telnet client. By default, the Telnet client service is disabled in Windows 7 and later. A shown in Figure 7, to manually enable the Telnet client service, go to **Select Control Panel** > **Programs and Features** > **Turn Windows features on or off**, and then select **Telnet Client**.

Figure 7 Enable the Telnet Client service



Control Panel ▸ All Control Panel Items ▸ Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Install a program from the network

Windows Features

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear check box. A filled box means that only part of the feature is turned

- ☐ Services for NFS
- ☐ Simple Network Management Protocol (SNMP)
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ☐ Subsystem for UNIX-based Applications
- ☑ Tablet PC Components
- ☑ Telnet Client
- ☑ Telnet Server
- ☐ TFTP Client
- ☑ Windows Gadget Platform
- ☐ Windows Process Activation Service

Procedure

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

# Enter system view and enable Telnet service.

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

# Enable scheme authentication to use AAA to authenticate VTY login users.

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

# Create the local user **abc**. Set the password to **hello12345**. Assign the **network-admin** user role to the user.

```
[Sysname] local-user abc
[Sysname-luser-manage-abc] password simple hello12345
[Sysname-luser-manage-abc] service-type telnet
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
[Sysname-luser-manage-abc] quit
```

Verifying the configuration

# Press **Win+R**, and enter **cmd** to open the Command Prompt window. Enter Telnet device management IP address, and then press **Enter**.

```
C:\Users\Administrator> telnet 192.168.3.1
```

# Enter the user account and press **Enter**. Enter the password and press **Enter**. The password is not displayed. Then, you are logged in to the system.

```
Login: abc
```

```
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.                    *
******************************************************************************

<Sysname>
```

Configuration files

```
#
 telnet server enable
#
line vty 0 63
 authentication-mode scheme
#
local-user abc
 password hash $h$6$I2Sg4Llj1qVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.

Configuring console login with local authentication

Introduction

The following information uses an example to describe the basic procedure for logging in to the device through a console port with local authentication.

Prerequisites

Enter the CLI. For more information, see Configuring console login.

Procedure

The local authentication methods include password authentication and scheme authentication.

Password authentication

# Enter system view.

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

# Configure password authentication for AUX line 0 (console port).

```
[Sysname] line aux 0
[Sysname-line-aux0] authentication-mode password
```

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

```
[Sysname-line-aux0] set authentication password simple hello12345
```

# Assign the **network-admin** user role to the user for the user to manage the device and access all resources.

```
[Sysname-line-aux0] user-role network-admin
```

# Return to system view.

```
[Sysname-line-aux0] quit
```

# Save the configuration.

```
[Sysname] save
```

Scheme authentication

# Enter system view.

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

# Configure scheme authentication for AUX line 0 (console port) with username/password authentication.

```
[Sysname] line aux 0
[Sysname-line-aux0] authentication-mode scheme
```

# Return to system view.

```
[Sysname-line-aux0] quit
```

# Create local user **Client**. Set the password to **hello12345** in plain text. Assign the **network-admin** user role to the user for the user to manage the device and access all resources.

```
[Sysname] local-user Client
```

```
[Sysname-luser-manage-Client] password simple hello12345
[Sysname-luser-manage-Client] authorization-attribute user-role network-admin
```

# Specify the **terminal** service type.

```
[Sysname-luser-manage-Client] service-type terminal
```

# Return to system view.

```
[Sysname-luser-manage-Client] quit
```

# Save the configuration.

```
[Sysname] save
```

Verifying the configuration

Log in to the device after configuration:

- For password authentication, enter password **hello12345** as prompted. You are logged in to the system. The password is not displayed.

  ```
  Line aux0 is available.

  Press ENTER to get started.
  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>
  ```

- For scheme authentication, enter username Client in the **Login** field and enter password **hello12345** as prompted. You area logged in to the system. The password is not displayed.

  ```
  Line aux0 is available.

  Press ENTER to get started.
  Login: Client
  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

- Password authentication:

```
#
line aux 0
```

```
 authentication-mode password
 user-role network-admin
 set authentication password hash $h$6$fHkW5VqkiATx1+QX$1c5xycW0hx3f9TJi2vMzCwUS
tFKCPNvM+M8KyCWPc1f1Q4nhm1SUDGp59LGlSHn+tsjjxpxEfA+00Y6yr00Ojg==
#
```

- Scheme authentication:

```
#
line aux 0
 authentication-mode scheme
#
local-user Client class manage
 password hash $h$6$nz1haYkZ7nMNDuD8$61zQWor52DYHpv2KFyCdVHX/d4W9VNRPfyEEU2zyuoB
oOZ5lIS8bLYqUFSjVlBncRIA25FIiz4Js13akTZ3SXw==
 service-type terminal
 authorization-attribute user-role network-admin
#
```

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.

Recovering the password of the console port

Introduction

The following information uses examples to describe the methods to recover the password of the console port. Different methods are suitable for different scenarios as follows:

- **Method 1**—Used when you forget only the password of the console port but Telnet or SSH login is available.
- **Methods 2 and 3**—Used when all passwords are forgotten, and you cannot log in to the device. In addition, the configuration file must be saved.
- **Methods 4**—Used when all passwords are forgotten, and you cannot log in to the device. In addition, the configuration file does not need to be saved.

Network configuration

None.

Procedure

IMPORTANT:

As a best practice, use method 1 to recover the password of the console port. If you forget all login passwords, use other methods.

Method 1

To change the password of the console port after you log in to the device through Telnet or SSH:

1. Log in to the device through Telnet or SSH.
2. Reconfigure the password. For more information, see "Configuring console login with local authentication."

Method 2

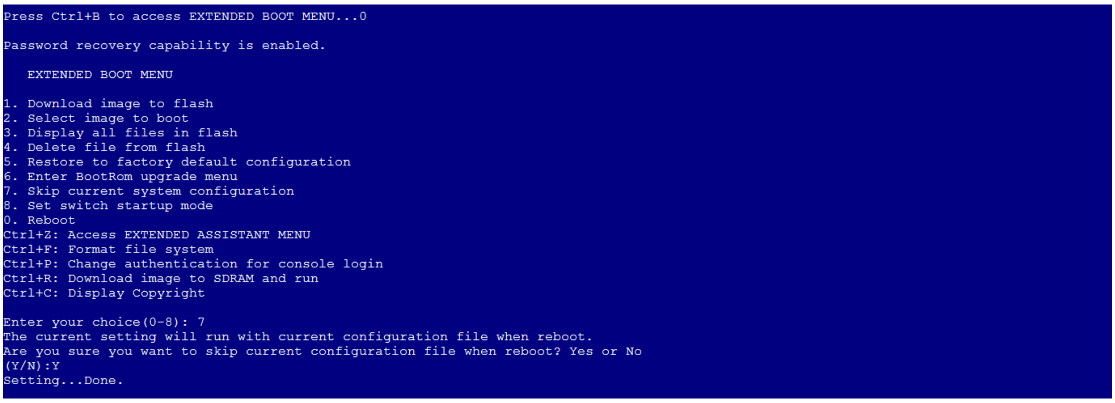
To skip the startup configuration file to start up the device from the BootWare menu and change the password of the console port:

NOTE:

BootWare menu varies by device model. This example uses the BootWare menu of the S5130 switch series.

1. Connect a configuration terminal to the console port of the device, and reboot the device.
2. During device reboot, press **Ctrl+B** to enter the BootWare menu. Then, select **Skip current system configuration** as shown in Figure 8.

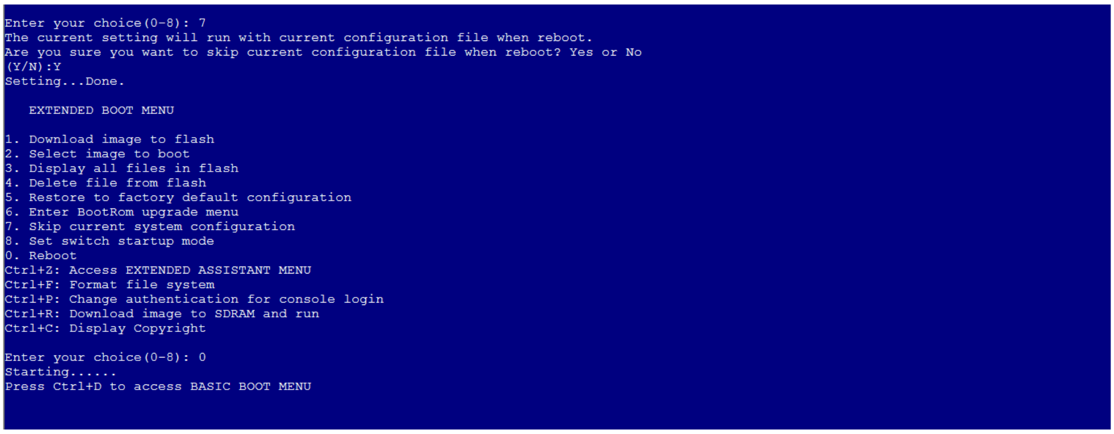
Figure 8 Entering the BootWare menu and selecting Skip current system configuration



```
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
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(0-8): 7
The current setting will run with current configuration file when reboot.
Are you sure you want to skip current configuration file when reboot? Yes or No
(Y/N):Y
Setting...Done.
```

3. Select **Reboot** to reboot the device as shown in Figure 9.

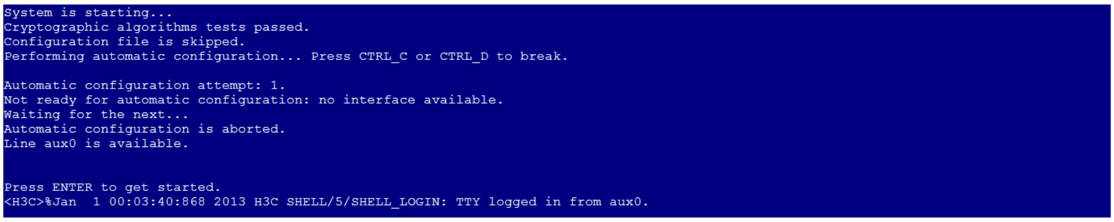
   Figure 9 Rebooting the device



```
Enter your choice(0-8): 7
The current setting will run with current configuration file when reboot.
Are you sure you want to skip current configuration file when reboot? Yes or No
(Y/N):Y
Setting...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
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(0-8): 0
Starting......
Press Ctrl+D to access BASIC BOOT MENU
```

4. During the reboot, press **Ctrl+C** or **Ctrl+D** to skip automatic configuration as shown in Figure 10.

   Figure 10 Skipping automatic configuration



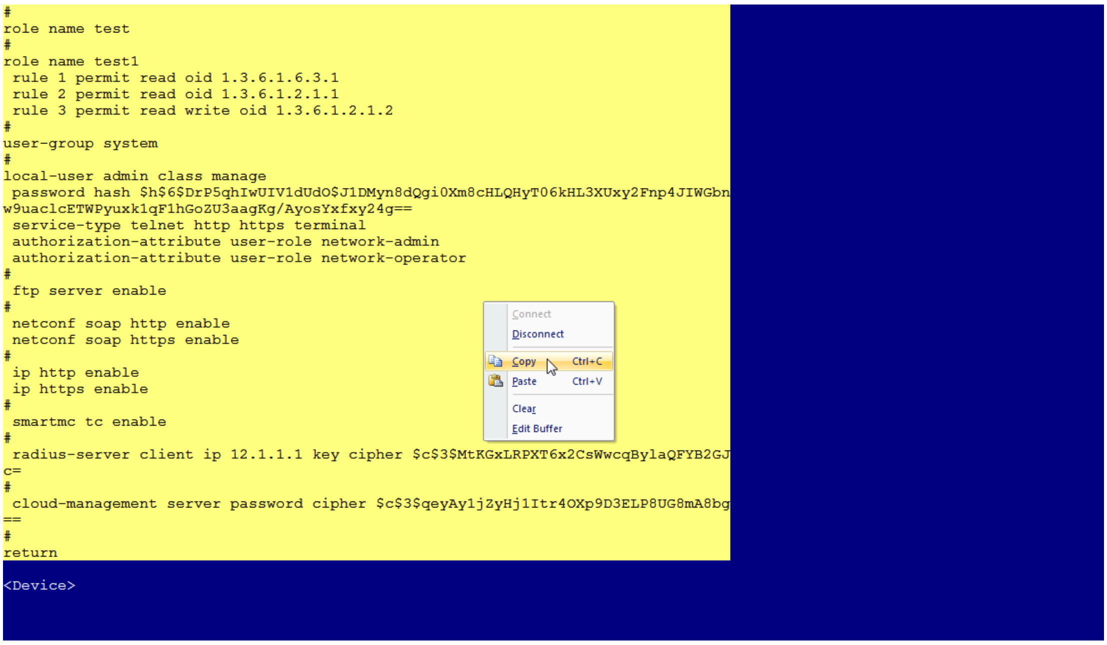
```
System is starting...
Cryptographic algorithms tests passed.
Configuration file is skipped.
Performing automatic configuration... Press CTRL_C or CTRL_D to break.

Automatic configuration attempt: 1.
Not ready for automatic configuration: no interface available.
Waiting for the next...
Automatic configuration is aborted.
Line aux0 is available.


Press ENTER to get started.
<H3C>%Jan  1 00:03:40:868 2013 H3C SHELL/5/SHELL_LOGIN: TTY logged in from aux0.
```

5. Press **Enter** to skip the startup configuration file to enter the CLI.
6. View the content of the startup configuration file. The *file-name* argument specifies the name of the startup configuration file.

   ```
   <Sysname> more startup.cfg
   ```

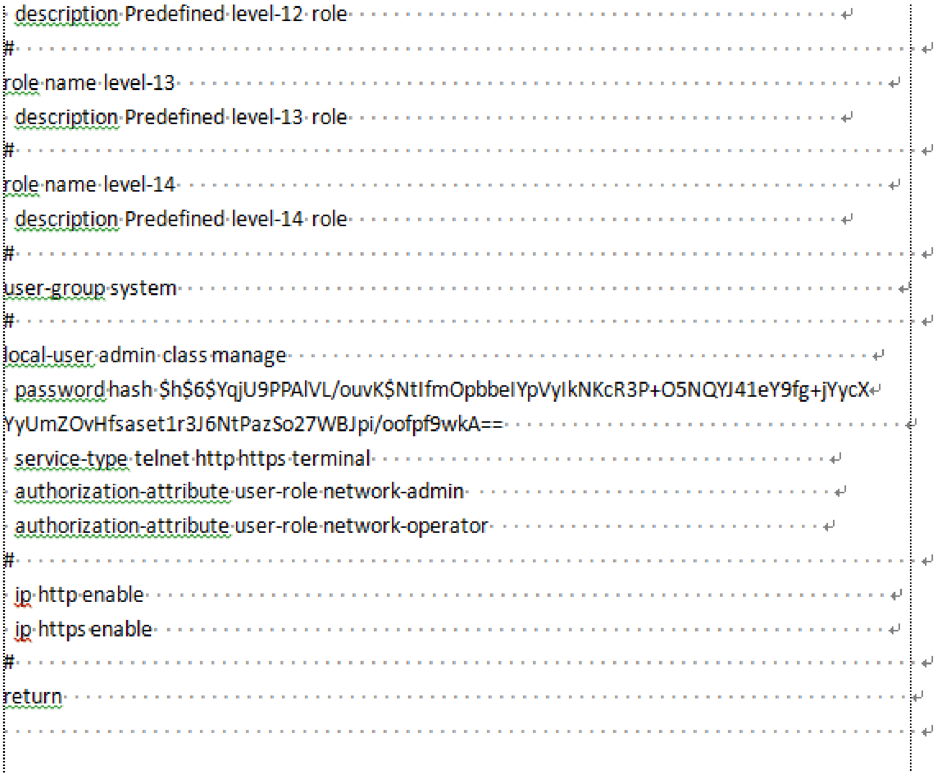
7. Select all command lines in the startup configuration file, copy them, and save them to a local file in TXT format, as shown in Figure 11 and Figure 12.

Figure 11 Copying the content in the startup configuration file



```
#
role name test
#
role name test1
 rule 1 permit read oid 1.3.6.1.6.3.1
 rule 2 permit read oid 1.3.6.1.2.1.1
 rule 3 permit read write oid 1.3.6.1.2.1.2
#
user-group system
#
local-user admin class manage
 password hash $h$6$DrP5qhIwUIV1dUdO$J1DMyn8dQgi0Xm8cHLQHyT06kHL3XUxy2Fnp4JIWGbn
w9uaclcETWPyuxk1qF1hGoZU3aagKg/AyosYxfxy24g==
 service-type telnet http https terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ftp server enable
#
 netconf soap http enable
 netconf soap https enable
#
 ip http enable
 ip https enable
#
 smartmc tc enable
#
 radius-server client ip 12.1.1.1 key cipher $c$3$MtKGxLRPXT6x2CsWwcqBylaQFYB2GJ
c=
#
 cloud-management server password cipher $c$3$qeyAy1jZyHj1Itr4OXp9D3ELP8UG8mA8bg
==
#
return

<Device>
```

Figure 12 Saving the content of the startup configuration file to a local file



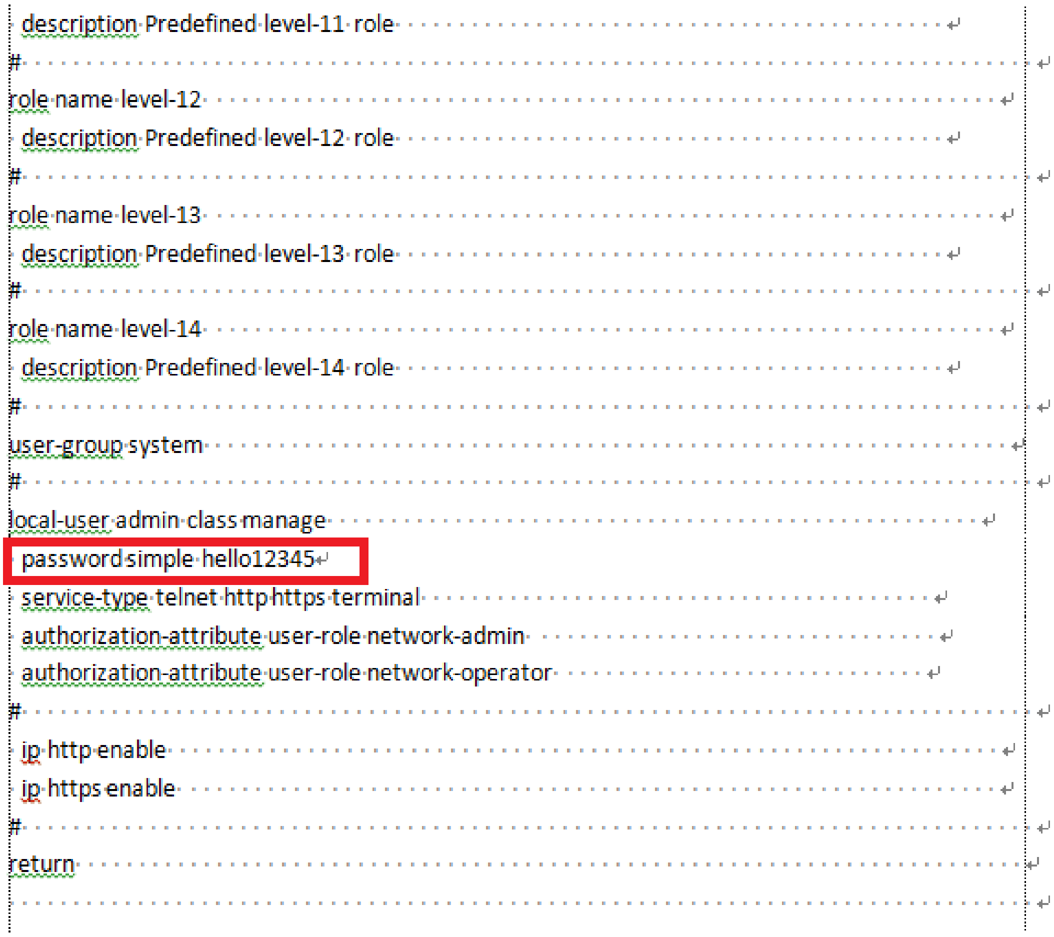
```
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash $h$6$YqjU9PPAlVL/ouvK$NtIfmOpbbeIYpVyIkNKcR3P+O5NQYJ41eY9fg+jYycX
YyUmZOvHfsaset1r3J6NtPazSo27WBJpi/oofpf9wkA==
 service-type telnet http https terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
 ip https enable
#
return
```

8. Modify the startup configuration file and delete the password or specify a new password, as shown in Figure 13. In this example, the new password is **hello12345**.

IMPORTANT:

The password for password authentication is configured in AUX line view. The password for scheme authentication is configured in local user view. This example modifies the password for scheme authentication.

Figure 13 Configuring a new password



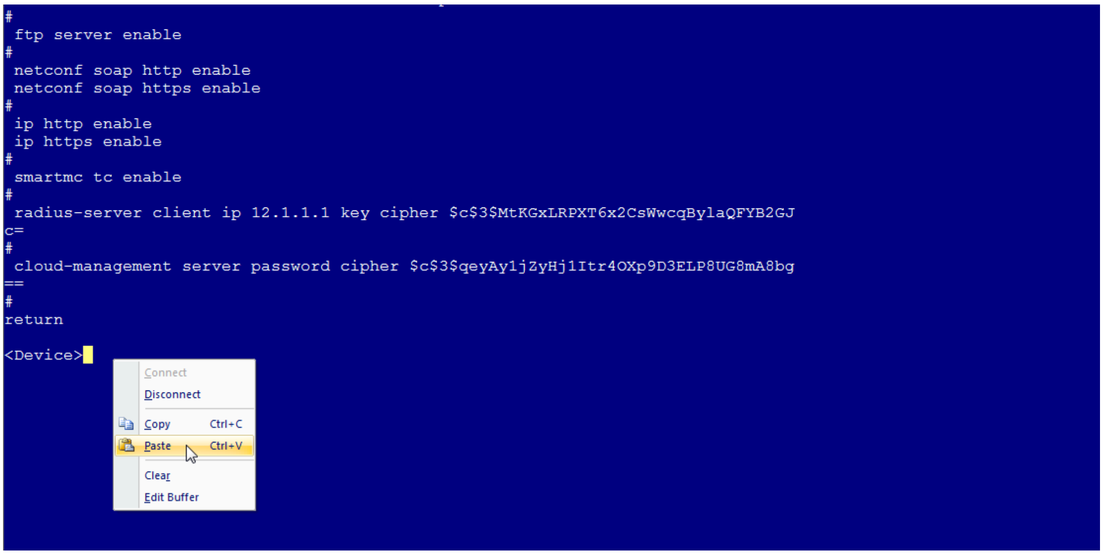
```
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password simple hello12345
 service-type telnet http https terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
 ip https enable
#
return
```

9. Enter system view.

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

10. Copy the content in the startup configuration file and paste them to the device, as shown in Figure 14.

Figure 14 Pasting the startup configuration file at the CLI



```
#
 ftp server enable
#
 netconf soap http enable
 netconf soap https enable
#
 ip http enable
 ip https enable
#
 smartmc tc enable
#
 radius-server client ip 12.1.1.1 key cipher $c$3$MtKGxLRPXT6x2CsWwcqBylaQFYB2GJ
c=
#
 cloud-management server password cipher $c$3$qeyAy1jZyHj1Itr4OXp9D3ELP8UG8mA8bg
==
#
return

<Device>
```

11. Save the configuration.

```
[Sysname] save
```

12. Return to user view and reboot the device.

```
[Sysname] quit
<Sysname> reboot
```

Method 3

To skip the startup configuration file to start up the device from the BootWare menu and roll back the running configuration:

1. Skip the startup configuration file to start up the device as described in method 2.

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

2. Roll back the running configuration to the configuration in a configuration file, for example, **startup.cfg**. Then, enter **N** to not save the running configuration.

```
[Sysname] configuration replace file startup.cfg
Current configuration will be lost, save current configuration? [Y/N]:N
Now replacing the current configuration. Please wait...
Succeeded in replacing current configuration with the file startup.cfg.
```

3. Reconfigure the password. For more information, see "Configuring console login with local authentication."

Method 4

To skip the startup configuration file to start up the device from the BootWare menu and save the running configuration:

device configuration to the factory defaults:

△ **CAUTION:**

The operations in this method clear all settings from the device. Make sure you fully understand the impacts of the operations on services.

1. Skip the startup configuration file to start up the device as described in method 2, and save the running configuration.

```
<Sysname> system-view
[Sysname] save
```

2. Reconfigure the password. For more information, see "Configuring console login with local authentication."

Configuration files

None.

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Configuration file management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.
- Configuration file management commands in the fundamentals command reference for the device.

Recovering the password for Telnet/Web login

Introduction

The following information uses an example to describe the method to use when a user forgets Telnet or Web login password.

Network configuration

None.

Procedure

When the password for Telnet login is forgotten

Log in to the device through the console port, and reconfigure the password for Telnet login. For more information, see "Configuring Telnet login."

When the password for Web login is forgotten

Log in to the device through the console port, and reconfigure the password for Web login as follows:

# Enter system view.

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

# Enter the view of the target Web user and set password to **hello12345**. This example uses user **client**.

```
[Sysname] local-user client
[Sysname-luser-manage-client] password simple hello12345
[Sysname-luser-manage-client] quit
```

# Save the configuration.

```
[Sysname] save
```

Configuration files

- Telnet login:

  For more information, see "Configuring Telnet login."

- Web login:

  ```
  #
  ip http enable
  #
  ip https enable
  #
  local-user client
   password hash $h$6$I2Sg4Llj1qVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
  XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
  ```

```
 service-type http https
 authorization-attribute user-role network-admin
#
```

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.

Configuration File Management Quick Start Configuration Guide

Contents

Restoring the factory defaults 1

Introduction 1
Restrictions and guidelines 1
Procedure 1
Related documentation 2

Backing up the configuration file 4

Introduction 4
Network configuration 4
Prerequisites 4
Procedure 4
Verifying the configuration 5
Related documentation 5

Skipping automatic configuration 6

Introduction 6
Network configuration 6
Prerequisites 6
Procedure 6
Related documentation 7

Restoring the factory defaults

Introduction

The following information uses an example to describe methods for restoring the factory defaults.

Restrictions and guidelines

Methods for restoring the factory defaults vary by device model.

Restoring the factory defaults removes all user-configured settings. After restoration, you can log in to the device only from the console port. SSH or Telnet login is not available. For more information about console login, see *Login Management Quick Start Configuration Guide*.

Procedure

- Execute the **restore factory-default** command and reboot the device.

  # Restore the device to the factory defaults.

  ```
  <Sysname> restore factory-default
  This command will restore the system to the factory default configuration and clear
  the operation data. Continue [Y/N]:y
  Restoring the factory default configuration. This process might take a few minutes.
  Please
  wait..................................................................
  .............................Done.
  Please reboot the system to place the factory default configuration into effect.
  ```

  # Reboot the device without saving the running configuration.

  ```
  <Sysname> reboot
  Start to check configuration with next startup configuration file, please
  wait.........DONE!
  Current configuration will be lost after the reboot, save current configuration?
  [Y/N]:n
  This command will reboot the device. Continue? [Y/N]:y
  Now rebooting, please wait...
  ```

- Remove configuration files and reboot the device.

  # Display the names of the current startup configuration file and the next-startup configuration files.

  ```
  <Sysname> display startup
  MainBoard:
   Current startup saved-configuration file: flash:/startup.cfg
   Next main startup saved-configuration file: flash:/startup.cfg
   Next backup startup saved-configuration file: NULL
  ```

  # Display the configuration files on the device.

  ```
  <Sysname> dir
  Directory of flash:
     0 -rw-        6244 Jan 08 2013 07:26:03   startup.cfg
     1 -rw-      136628 Jan 08 2013 07:26:03   startup.mdb
  ```

```
   2 -rw-       58704 Jan 03 2013 07:56:22   diag_H3C_20130103-005605.tar.gz
...
```

# Delete the next-startup configuration file.

```
<Sysname> delete /unreserved startup.cfg
The file cannot be restored. Delete flash:/startup.cfg?[Y/N]:y
Deleting a file permanently will take a long time. Please wait...
%Delete file flash:/startup.cfg...Done.
```

# Reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:n
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

- Delete the next-startup configuration file and reboot the device.

IMPORTANT:

- By default, this method permanently deletes the next-startup configuration files from all IRF member devices. To delete the configuration file only from the master device, disable automatic system-wide next-startup configuration file operations.
- Reboot the device without saving the running configuration.

# Display the names of the current startup configuration file and the next-startup configuration files.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

# Delete the main next-startup configuration file.

```
<Sysname> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:Y
```

If the device has a backup next-startup configuration file, execute the **reset saved-configuration backup** command to delete the backup next-startup configuration file.

# Reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration?
[Y/N]:n
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Related documentation

- Configuration file management in the fundamentals configuration guide for the device.

- Configuration file management commands in the fundamentals command reference for the device.
- Device management in the fundamentals configuration guide for the device.
- Device management commands in the fundamentals command reference for the device.
- File system management in the fundamentals configuration guide for the device.
- File system management commands in the fundamentals command reference for the device.

Backing up the configuration file

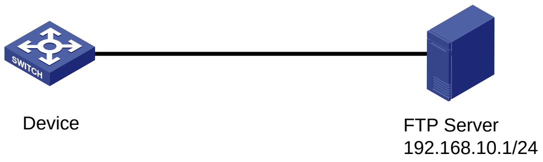
Introduction

The following information uses an example to describe the basic procedure for configuration file backup.

Network configuration

As shown in Figure 1, back up the current configuration file of the device to the FTP server.

Figure 1 Network diagram



Prerequisites

Make sure the device can reach the FTP server.

Procedure

# Save the running configuration to a configuration file. By default, the name of the configuration file is **startup.cfg**.

```
<Sysname> 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...
Saved the current configuration to mainboard device successfully.
```

The output shows that the device has a configuration file named **starup.cfg** by default.

# Upload the **startup.cfg** file to the FTP server.

```
<Sysname> ftp 192.168.10.1
Press CTRL+C to abort.
Connected to 192.168.10.1 (192.168.10.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.10.1:(none)): root
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp> binary
200 Type is Image (Binary)
```

```
ftp> put start.cfg
ftp: No such file or directory
ftp> put startup.cfg
227 Entering Passive Mode (192,168,10,1,235,54)
150 "D:\temp\startup.cfg" file ready to receive in IMAGE / Binary mode
.
226 Transfer finished successfully.
4326 bytes sent in 0.003 seconds (1.49 Mbytes/s)
```

Verifying the configuration

# Display uploaded configuration files.

```
ftp> dir
227 Entering Passive Mode (192,168,10,1,252,152)
1 File Listing Follows in ASCII mode
-rwxrwxrwx   1 noone    nogroup     4326 Sep  2 14:00 startup.cfg
```

The output shows that the **startup.cfg** file has been uploaded to the FTP server.

Related documentation

- Configuration file management in the fundamentals configuration guide for the device.
- Configuration file management commands in the fundamentals command reference for the device.
- FTP and TFTP configuration in the fundamentals configuration guide for the device.
- FTP and TFTP commands in the fundamentals command reference for the device.

Skipping automatic configuration

Introduction

When the device starts up without a valid next-startup configuration file, the device searches the root directory of its default file system for the autocfg.py, autocfg.tcl, and autocfg.cfg files. Only one of files might exist in the root directory. If any one of the files exists, the device loads the file. If none of the files exists, the device uses the automatic configuration feature to obtain a set of configuration settings.

With the automatic configuration feature, the device can automatically obtain a set of configuration settings at startup. Automatic configuration simplifies network configuration and maintenance.

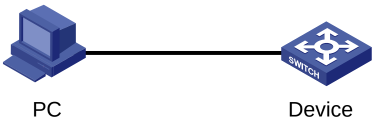
If the device is not deployed in a large-scale network, skip automatic configuration.

The following information uses an example to describe the basic procedure for skipping automatic configuration.

Network configuration

As shown in Figure 2, the device starts up with the initial configuration and skips automatic configuration.

Figure 2 Network diagram



Prerequisites

When the device starts up with the initial configuration, log in to the device from the console port. For more information about console login, see *Login Management Quick Start Configuration Guide*.

Procedure

# Power on the device.

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU
Press Ctrl+T to start heavy memory test

*********************************************************************************
*                                                                               *
*                  H3C S5570S-28S-HPWR-EI  BOOTROM, Version 105                 *
*                                                                               *
*********************************************************************************
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.

Creation Date         : Jul  6 2021
```

```
CPU Clock Speed      : 1000MHz
Memory Type          : DDR4 SDRAM
Memory Size          : 1024MB
Memory Speed         : 800MHz
CPLD Version         : 001
PCB Version          : Ver.A
Mac Address          : b04414cd47a4


BootRom Validating...
Press Ctrl+B to access EXTENDED BOOT MENU...0
Loading the main image files...
Loading file flash:/s5570s_ei-cmw710-system-e1105p09.bin........................
.......................................................Done.
Loading file flash:/s5570s_ei-cmw710-devkit-e1105p09.bin.....Done.
Loading file flash:/s5570s_ei-cmw710-boot-e1105p09.bin.........Done.

Image file flash:/s5570s_ei-cmw710-boot-e1105p09.bin is self-decompressing......
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................Done.
System is starting...
Cryptographic algorithms tests passed.

Startup configuration file doesn't exist or is invalid.
Performing automatic configuration... Press CTRL_C or CTRL_D to break.

Automatic configuration attempt: 1.
Not ready for automatic configuration: no interface available.
Waiting for the next...

Automatic configuration attempt: 2.
Not ready for automatic configuration: no interface available.
Waiting for the next...
```

Press **CTRL+D** or **Ctrl+C** to stop automatic configuration and enter the Comware system.

Related documentation

- Automatic configuration in the fundamentals configuration guide for the device.
- Automatic configuration commands in the fundamentals command reference for the device.

Software Upgrade Quick Start Configuration Guide

Contents

Upgrading software at the CLI ··· 1

- Introduction ··· 1
- Network configuration ··· 1
- Restrictions and guidelines ··· 1
- Prerequisites ··· 1
- Procedure ··· 5
    - Configuring IP addresses for interfaces ··· 5
    - Configuring an IP address for the PC ··· 5
    - Viewing the current version information ··· 7
    - Viewing the free storage space ··· 7
    - Upgrading software ··· 8
- Verify the configuration ··· 8
- Configuration files ··· 9
- Related documentation ··· 9

Upgrade software through the BootWare menu and Xmodem ··· 10

- Introduction ··· 10
- Network configuration ··· 10
- Restrictions and guidelines ··· 10
- Prerequisites ··· 10
- Procedure ··· 11
    - Viewing the current version information ··· 11
    - Accessing the BootWare menu ··· 11
    - Modifying the terminal baud rate ··· 12
    - Upgrading software ··· 14
- Verify the configuration ··· 16
- Configuration files ··· 16
- Related documentation ··· 17

Upgrading software at the CLI

Introduction

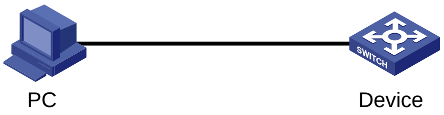
The following information uses an example to describe the basic procedure for upgrading software at the CLI.

Network configuration

As shown in Figure 1, the PC and the device are connected through a configuration cable.

Configure the PC as a file server and enable the TFTP server on it. Configure the device as a TFTP client, download the upgrade file to the device through TFTP, and upgrade the device software.

Figure 1 Network diagram



Restrictions and guidelines

Use the release notes for the upgrade software version to evaluate the upgrade impact on your network and verify the compatibility of the upgrade software with the current software version.

An upgrade requires the device to reboot. Please upgrade software during off-peak hours.

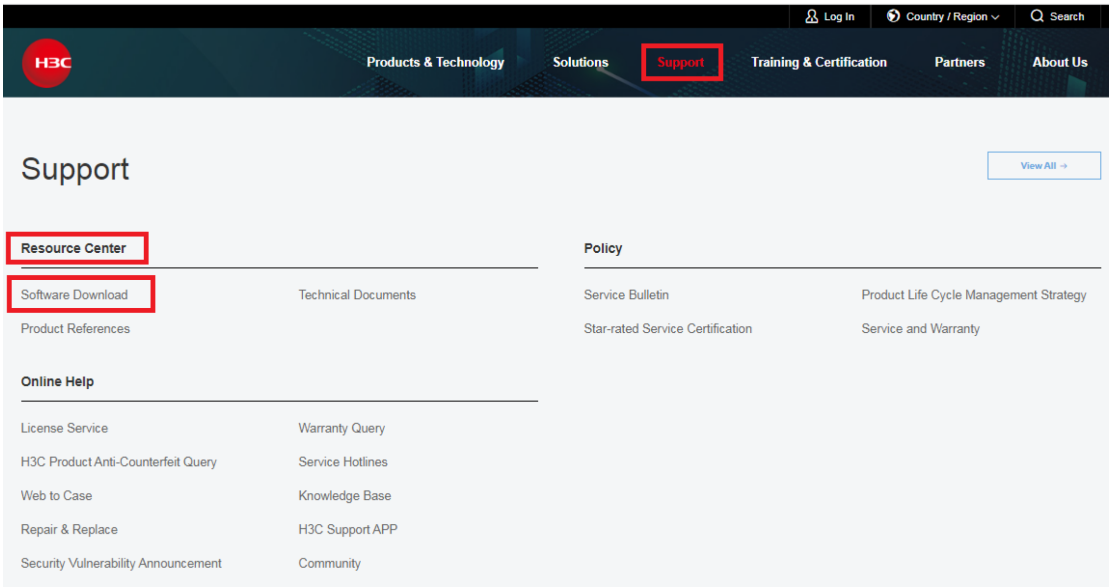
Prerequisites

Obtaining the software image files

You can obtain the upgrade file by using either of the following methods:

- Log in to http://www.h3c.com/en, select **Support** > **Resource Center** > **Software Download**, find the target device, and download the upgrade file.

Figure 2 Downloading the upgrade file



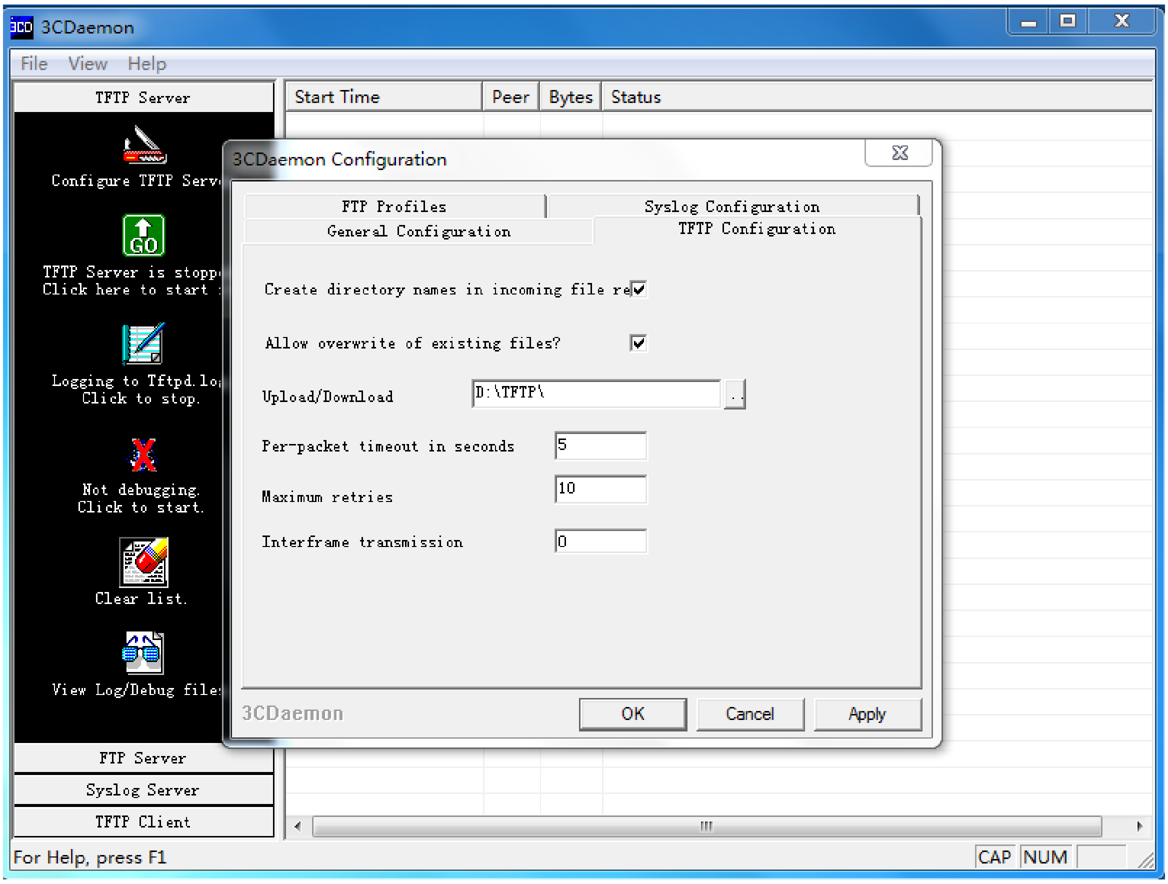
- Contact H3C Support to obtain the upgrade file.

Configuring the file server

The device can function as an FTP, TFTP, or SFTP client. In this example, the device functions as a TFTP client.

# Enable the FTP server on the PC (3CDaemon, in this example), set the upload/download path, and enable the TFTP service.

Figure 3 Setting the upload/download path



Create directory names in incoming file re ☑

Allow overwrite of existing files? ☑

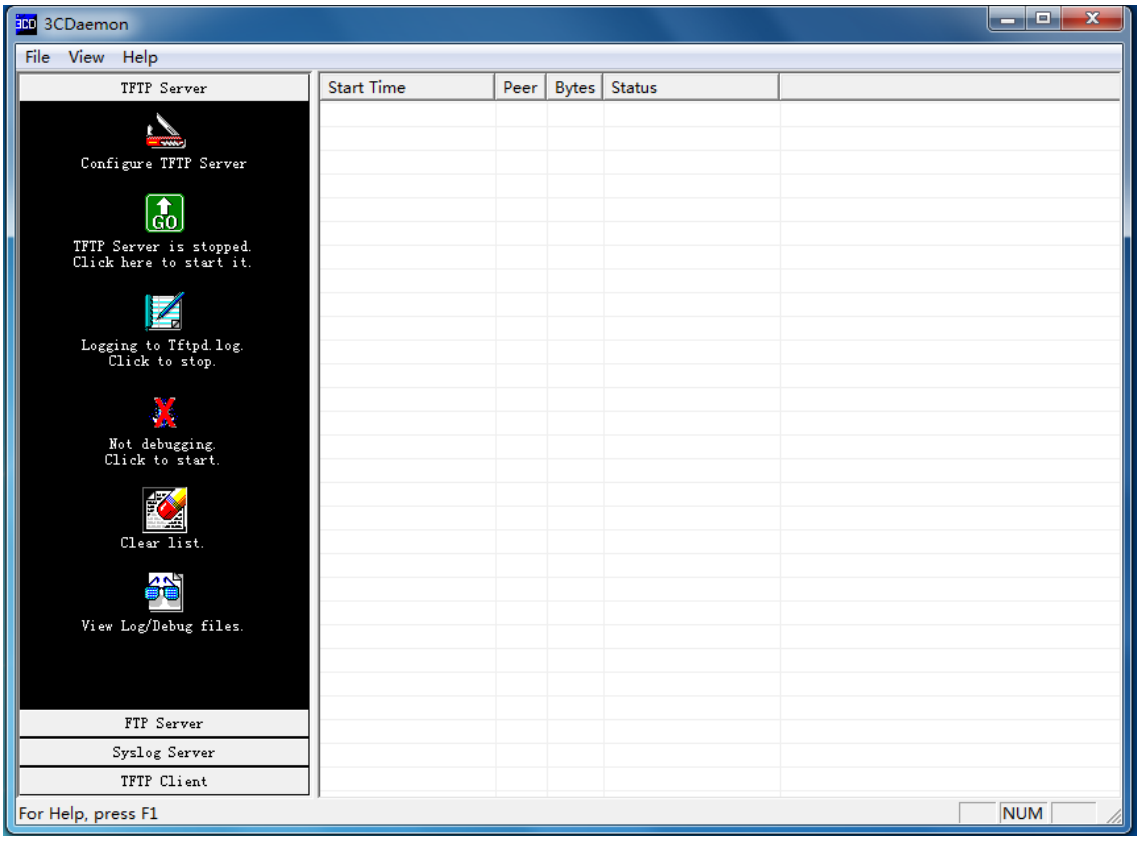
Upload/Download D:\TFTP\

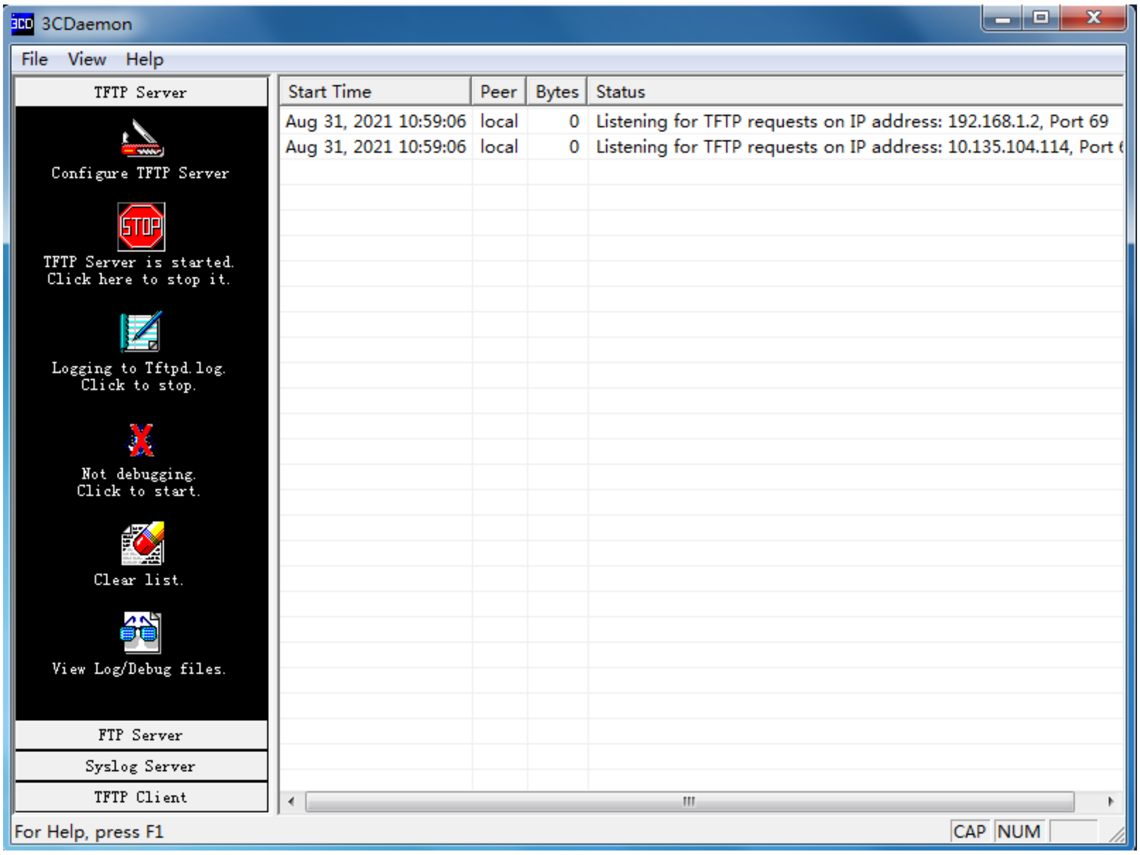
Per-packet timeout in seconds 5

Maximum retries 10

Interframe transmission 0

Figure 4 Enabling the TFTP service





Start Time	Peer	Bytes	Status
Aug 31, 2021 10:59:06	local	0	Listening for TFTP requests on IP address: 192.168.1.2, Port 69
Aug 31, 2021 10:59:06	local	0	Listening for TFTP requests on IP address: 10.135.104.114, Port

Procedure

Configuring IP addresses for interfaces

# Create VLAN 99.

```
<Switch> system-view
[Switch] vlan 99
[Switch-vlan99] quit
```

# Create VLAN interface 99.

```
[Switch] interface vlan-interface 99
```

# Assign IP address 192.168.1.1/24 to VLAN interface 99.

```
[Switch-Vlan-interface99] ip address 192.168.1.1 24
[Switch-Vlan-interface99] quit
```

# Enter the view of the interface that connects to the PC, GigabitEthernet 1/0/1 in this example.

```
[Switch] interface gigabitethernet 1/0/1
```

# Configure GigabitEthernet 1/0/1 to operate in Layer 2 mode.

```
[Switch-GigabitEthernet1/0/1] port link-mode bridge
```

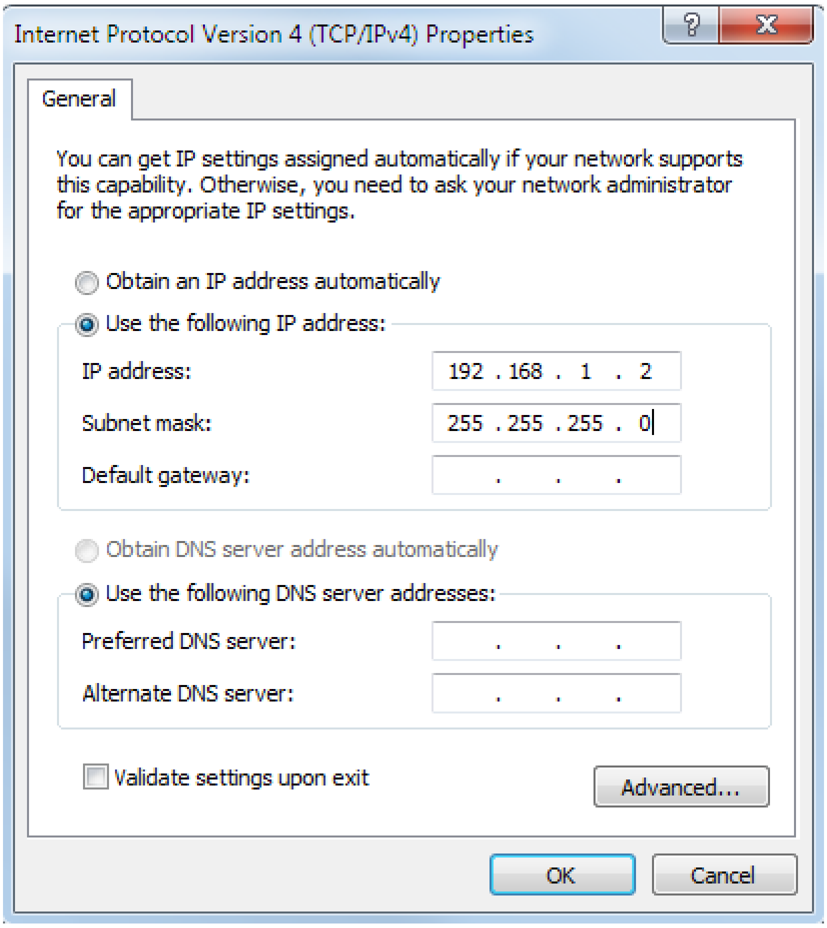
# Assign GigabitEthernet 1/0/1 to VLAN 99.

```
[Switch-GigabitEthernet1/0/1] port access vlan99
[Switch-GigabitEthernet1/0/1] quit
```

Configuring an IP address for the PC

# Assign IP address 192.168.1.2/24 to the PC.

Figure 5 Assigning IP address 192.168.1.2/24 to the PC



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

# Open the **Run** window by using the Win + R short keys, enter **cmd** in the **Open** field, and ping the device in the Command window.

```
C:\ Documents and Setting\Administrator> ping 192.168.1.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=31ms TTL=253
Reply from 192.168.1.1: bytes=32 time=30ms TTL=253
Reply from 192.168.1.1: bytes=32 time=30ms TTL=253
Reply from 192.168.1.1: bytes=32 time=30ms TTL=253

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 31ms, Average = 30ms
```

# Ping the TFTP server from the device.

```
<Switch> ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=10.701 ms
56 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=2.678 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=2.282 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=1.617 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=1.701 ms
```

```
--- Ping statistics for 192.168.1.2 ---
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.
```

Viewing the current version information

# View the current version information. You can check whether the upgrade succeeds by comparing the version information before and after the upgrade.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
…
```

Viewing the free storage space

# Execute the **dir** command to verify that the device has sufficient space for the new system software image. Typically, the storage space should be twice the size of the upgrade file.

```
<Switch> dir
Directory of flash:
   0 drw-      707584 Jan 29 2013 05:41:21   123.bin
   1 drw-       12639 Jan 29 2013 05:41:21   patch.bin
   2 drw-    48866304 Jan 02 2013 08:30:11   r6126p20.ipe
   3 -rw-         591 Jan 01 2013 03:31:14   serverkey
   4 -rw-        6304 Feb 02 2013 06:58:55   startup.cfg
   5 -rw-      159335 Feb 02 2013 06:58:55   startup.mdb
   6 -rw-           0 Jan 02 2013 06:19:27   topology.dba
   7 drw-           - Jan 02 2013 05:32:24   versionInfo
…
251904 KB total (25052 KB free)
```

# If the free storage space is not sufficient, delete unused files.

```
<Switch> delete /unreserved patch.bin
The file cannot be restored. Delete flash:/patch.bin? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/123.bin...Done.
```

NOTE:

- The .ipe file will be decompressed into multiple .bin files. Make sure the storage space is sufficient for storing the decompressed files. Typically, the storage space should be twice the size of the upgrade files.
- To delete a file permanently, use the **`delete /unreserved`** command. If you use the **`delete`** command, the file is moved to the recycle bin and still occupies the storage space. To release the storage space, you must execute the **`reset recycle-bin`** command in the file's original directory.

Upgrading software

# Place the upgrade image file **switch.ipe** in the upload/download path on the TFTP server.

# Download the upgrade image file to the device through TFTP.

```
<Switch> tftp 192.168.1.2 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 the **switch.ipe** file as the main startup file for the device.

```
<Switch> boot-loader file flash:/switch.ipe all main
```

# After the file is decompressed, the system prompts you to delete the file. If the file will be used for rollback, enter N.

```
<Switch> Do you want to delete flash:/switch.ipe now? [Y/N]:N
```

# Reboot the device.

```
<Switch> reboot
```

Verify the configuration

# Execute the **`display version`** command to verify that the software has been upgraded.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
…
```

# 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

```
#
interface vlan-interface 99
ip address 192.168.1.1 24
#
interface gigabitethernet 1/0/1
port link-mode bridge
port access vlan 99
#
```

Related documentation

- Software upgrade configuration in the fundamentals configuration guide for the device.
- Software upgrade commands in the fundamentals command reference for the device

Upgrade software through the BootWare menu and Xmodem

Introduction

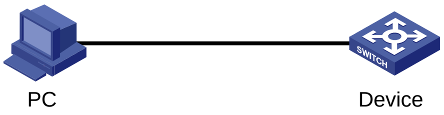
The following information uses an example to describe the basic procedure for upgrading software through the BootWare menu and Xmodem.

Network configuration

As shown in Figure 2, the PC and the device are connected through a configuration cable.

Download the upgrade file to the device through Xmodem, and upgrade the device software.

Figure 2 Network diagram



Restrictions and guidelines

Use the release notes for the upgrade software version to evaluate the upgrade impact on your network and verify the compatibility of the upgrade software with the current software version.

An upgrade requires the device to reboot. Please upgrade software during off-peak hours.

Xmodem is slow to transfer files. As a best practice, use a network cable to transfer files (see "Upgrading software at the CLI").

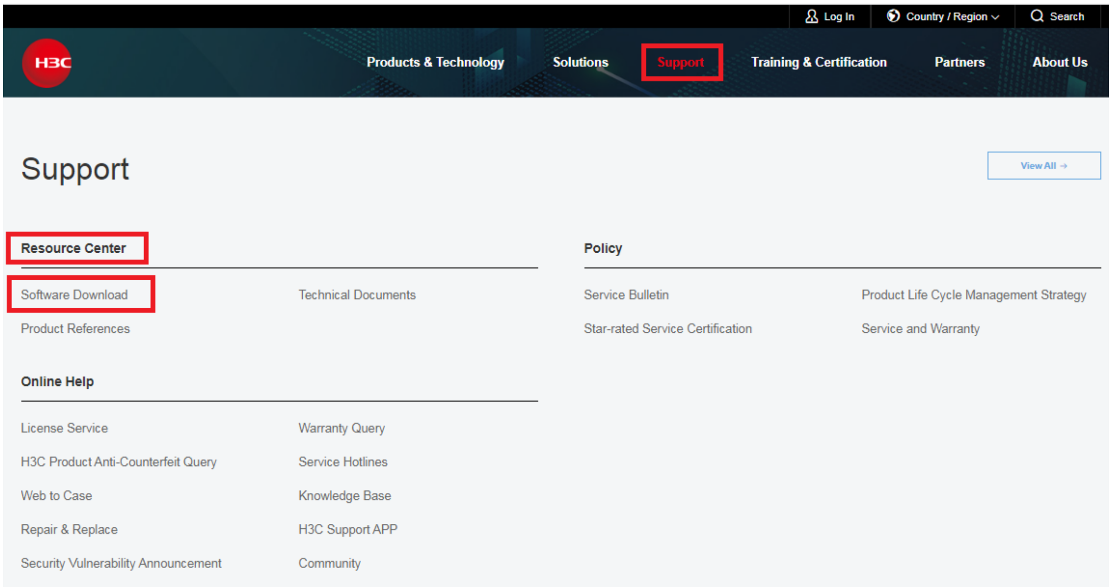
Prerequisites

Obtaining the software image files

You can obtain the upgrade file by using either of the following methods:

- Log in to http://www.h3c.com/en, select **Support** > **Resource Center** > **Software Download**, find the target device, and download the upgrade file.

Figure 3 Downloading the upgrade file



- Contact H3C Support to obtain the upgrade file.

Downloading management software

Download management software. This example uses HyperTerminal.

Procedure

Viewing the current version information

# View the current version information. You can check whether the upgrade succeeds by comparing the version information before and after the upgrade.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
…
```

Accessing the BootWare menu

# Press **Ctrl+B** after the "Press Ctrl+B to enter extended boot menu..." message appears upon device startup.

```
Press Ctrl+B to enter extended boot menu...
BootWare password: Not required. Please press Enter to continue.
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
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 **1** to download the image file to the flash memory.

```
Enter your choice(0-8): 1
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu
```

# Enter **3** to set the Xmodem download baud rate.

```
Enter your choice(0-3): 3
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu
```

# Select an appropriate download rate, for example, enter **5** to select 115200 bps.

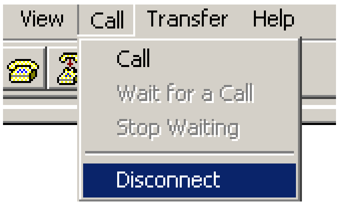
```
Enter your choice(0-5): 5
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

Modifying the terminal baud rate

Set the serial port on the terminal to use the same baud rate as the console port.

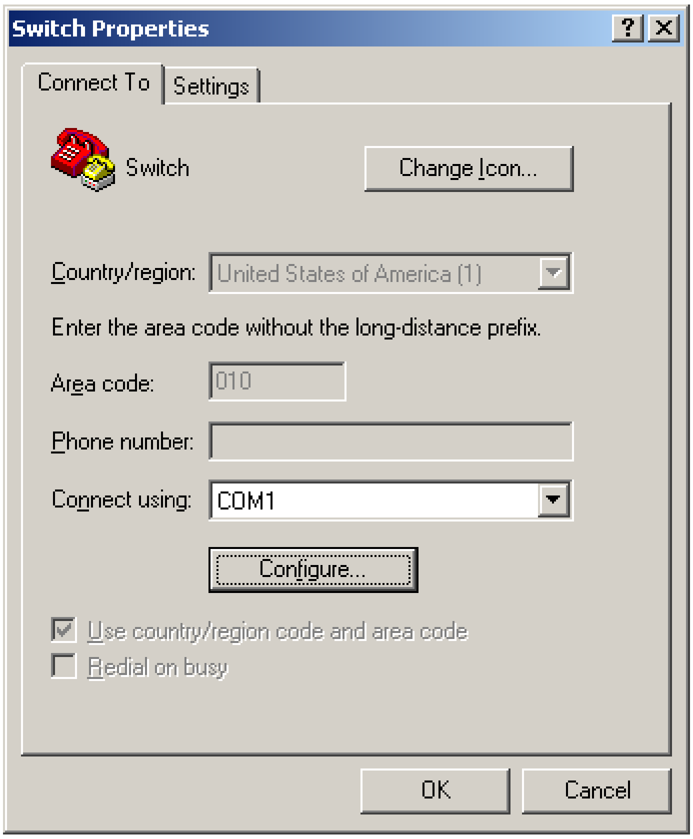
1. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 4 Disconnecting the terminal from the switch



2. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 5 Properties dialog box



Switch

Country/region: United States of America (1)

Enter the area code without the long-distance prefix.

Area code: 010

Phone number:

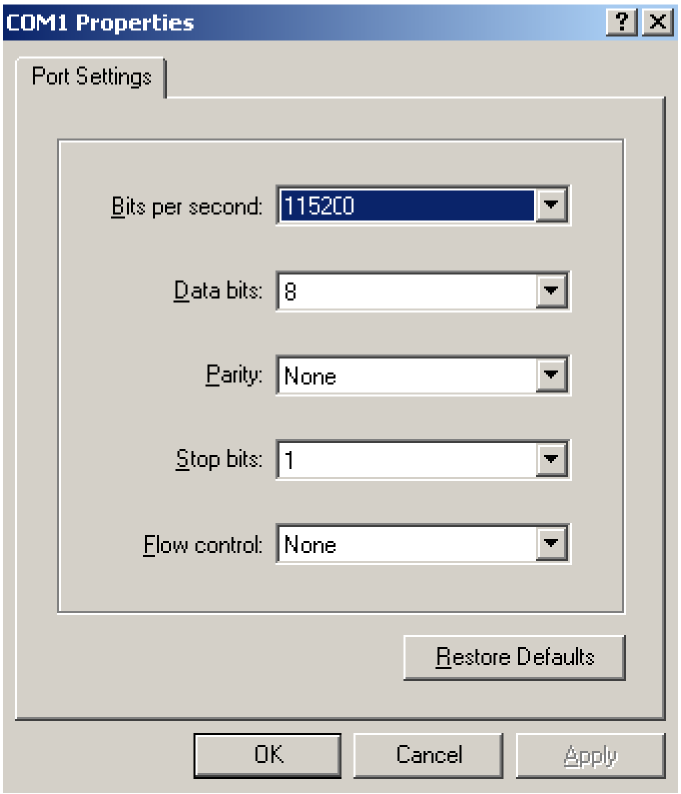
Connect using: COM1

☑ Use country/region code and area code

□ Redial on busy

3. Select **115200** from the **Bits per second** list, and click **OK**.

Figure 6 Modifying the baud rate



Bits per second: 115200

Data bits: 8

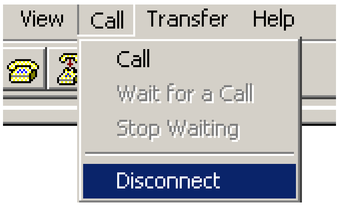
Parity: None

Stop bits: 1

Flow control: None

4. Select **Call** > **Call** to re-establish the connection.

Figure 7 Re-establishing the connection



Upgrading software

1. Press **Enter**. The following message appears:

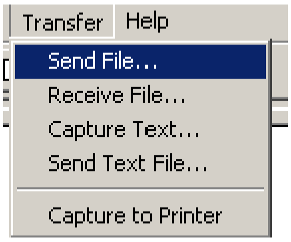
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

2. Enter **Y** to start downloading the file. (To return to the BootWare menu, enter **N**.)

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCC
```

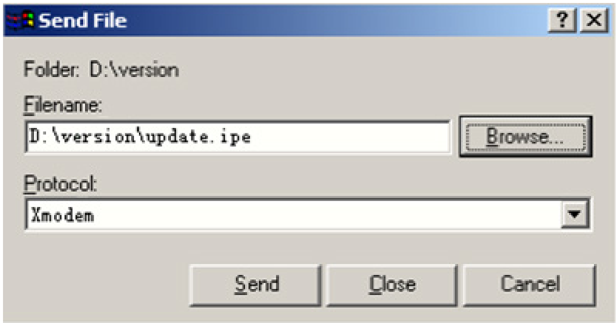
3. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 8 Transfer menu



4. In the dialog box that appears, click **Browse…** to select the image file, and select **Xmodem** from the **Protocol** list.

Figure 9 File transmission dialog box



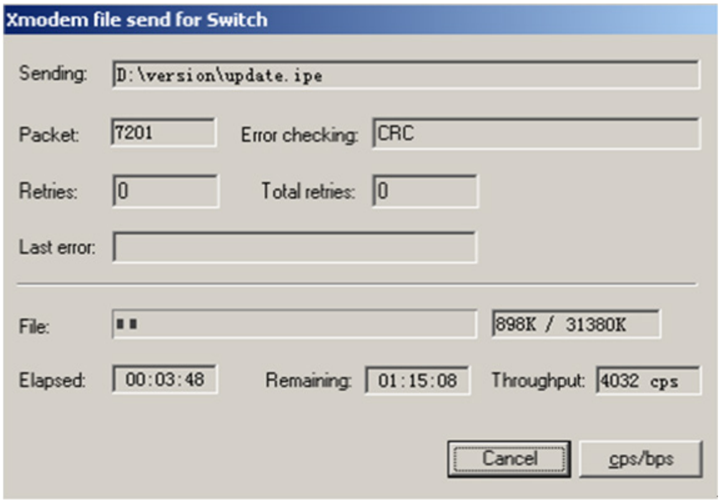
Folder: D:\version

Filename: D:\version\update.ipe

Protocol: Xmodem

5. Click **Send**. The following dialog box appears:

Figure 10 File transfer progress



Xmodem file send for Switch

Sending: D:\version\update.ipe

Packet: 7201 Error checking: CRC

Retries: 0 Total retries: 0

Last error:

File: 898K / 31380K

Elapsed: 00:03:48 Remaining: 01:15:08 Throughput: 4032 cps

6. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the image file. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
Load File name  : boot.bin       // Set the name of the boot image file
Free space: 470519808 bytes
Writing flash...................................................................
.............
Done!
The system-update.bin image is self-decompressing...
Load File name  : system.bin      // Set the name of the system image file
Free space: 461522944 bytes
Writing flash...................................................................
.............
Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

NOTE:

If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid.

7. Restore the baud rate of the HyperTerminal to 9600 bps (see "Modifying the terminal baud rate"). If the baud rate is 9600 bps, skip this step.
8. Press **Enter** to access the BootWare menu.

```
   EXTENDED BOOT MENU

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 default boot storage medium
0. Reboot
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): 0
```

9. Enter **0** to reboot the system with the new software images.

Verify the configuration

# Execute the **display version** command to verify that the software has been upgraded.

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
…
```

# 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

```
#
interface vlan-interface 99
ip address 192.168.1.1 24
#
interface gigabitethernet 1/0/1
port link-mode bridge
port access vlan 99
#
```

Related documentation

- Software upgrade configuration in the fundamentals configuration guide for the device.
- Software upgrade commands in the fundamentals command reference for the device.

Device Management Quick Start Configuration Guide

Contents

Configuring the device name and system time ··· 1

Introduction ··· 1

Procedure ··· 1

Configuring the device name ··· 1

Configuring the system time ··· 1

Verifying the configuration: ··· 2

Configuration files ··· 2

Related documentation ··· 2

Scheduling a device reboot ··· 3

Introduction ··· 3

Procedure ··· 3

Configuring the device to reboot at a specific date and time ··· 3

Configuring the device to reboot after a period of time ··· 3

Configure the device to reboot at the specified time every day ··· 3

Verifying the configuration ··· 4

Configuration files ··· 4

Related documentation ··· 4

Configuring the device name and system time

Introduction

The following information uses examples to describe the basic procedure for configuring the device name and system time.

The device can use one of the following methods to obtain the system time:

- Uses the locally set system time, and then uses the clock signals generated by its built-in crystal oscillator to maintain the system time.
- Periodically obtains the UTC time from an NTP or PTP source, and then uses the UTC time, time zone, and daylight saving time to calculate the system time. For more information about NTP and PTP, see the network management and monitoring configuration guide for the device.

The system time calculated by using the UTC time from a time source is more precise.

NOTE:

Support for PTP depends on the device model.

Procedure

Configuring the device name

# Enter system view.

```
<Device> system-view
```

# Set the device name to **abcd**.

```
[Device] sysname abcd
[adcd]
```

Configuring the system time

Using the locally set system time

# Enter system view.

```
<Device> system-view
```

# Configure the device to use the locally set system time.

```
[Device] clock protocol none
```

# Return to user view, and set the local system time to 11:08:00 2021/09/01.

```
[Device] quit
<Device> clock datetime 11:8 2021/9/1
```

Obtaining the system time through NTP

# Enter system view.

```
<Device> system-view
```

# Specify NTP for obtaining the system time.

```
[Device] clock protocol ntp
```

Obtaining the system time through PTP

# Enter system view.

```
<Device> system-view
```

# Specify PTP for obtaining the system time.

```
[Device] clock protocol ptp
```

Verifying the configuration:

# Display the current system time.

```
[Device] display clock
11:08:00.258 UTC Wed 01/09/2021
```

The command output shows the system time in *hour*:*minute*:*second*.*millisecond* format.

Configuration files

- Configure the device name.

  ```
  #
   sysname abcd
  #
  ```

- Use the locally set system time.

  ```
  #
   clock datetime 11:8 2021/9/1
   clock protocol none
  #
  ```

- Obtain the system time through NTP.

  ```
  #
   clock protocol ntp
  #
  ```

- Obtain the system time through PTP.

  ```
  #
   clock protocol ptp
  #
  ```

Related documentation

- Device management configuration in the fundamentals configuration guide for the device.
- Device management commands in the fundamentals command reference for the device.

Scheduling a device reboot

Introduction

The following information uses examples to describe the basic procedure for scheduling a device reboot.

You can schedule a device reboot as follows:

- Configure the device to reboot at a specific date and time.
- Configure the device to reboot after a period of time.
- Configure the device to reboot at the specified time every day.

Procedure

Configuring the device to reboot at a specific date and time

# Configure the device to reboot at 12:00 p.m. This example assumes that the current time is 11:00 a.m. on September 1, 2021.

```
<Device> scheduler reboot at 12:00
Reboot system at 12:00:00 01/09/2021 (in 1 hours and 0 minutes). Confirm? [Y/N]:Y
```

Configuring the device to reboot after a period of time

# Configure the device to reboot after 88 minutes. This example assumes that the current time is 11:00 a.m. on September 1, 2021.

```
<Device> scheduler reboot delay 88
Reboot system at 12:28 01/09/2021(in 1 hours and 28 minutes). Confirm? [Y/N]:Y
```

### Configure the device to reboot at the specified time every day

# Enter system view.

```
<Device> system-view
```

# Create a job named **reboot** and assign the **`reboot`** command to the job.

```
[Device] scheduler job reboot
[Device-job-reboot] command 1 reboot
```

# Exit to system view.

```
[Device-job-reboot] quit
```

# Create a schedule named **schedule-reboot**, and assign job **reboot** to it for it to execute device reboot at 23:00 every day.

```
[Device] scheduler schedule schedule-reboot
[Device-schedule-schedule-reboot] job reboot
[Device-schedule-schedule-reboot] time repeating at 23:00
```

# Exit to system view.

```
[Device-schedule-schedule-reboot] quit
```

# Save the configuration.

```
[Device] save
```

Verifying the configuration

# Display the automatic reboot schedule.

```
<Device> display scheduler reboot
System will reboot at 12:28 01/09/2021 (in 1 hours and 28 minutes).
```

# Display schedule information.

```
[Device-schedule-schedule-reboot] display scheduler schedule
Schedule name        : schedule-reboot
Schedule type        : Run on every day at 23:00:00
Start time           : Wed Sep 01 11:00:00 2021
Last execution time  : Yet to be executed
-----------------------------------------------------------------------
Job name                                          Last execution status
reboot                                            -NA-
```

# Display job configuration information.

```
[Device] display scheduler job
Job name: reboot
 reboot
```

Configuration files

Configure the device to reboot at 23:00 every day.

```
#
scheduler job reboot
 command 1 reboot
#
scheduler schedule schedule-reboot
 user-role network-operator
 user-role network-admin
 job reboot
 time repeating at 23:00
#
```

Related documentation

- Device management configuration in the fundamentals configuration guide for the device.
- Device management commands in the fundamentals command reference for the device.

NTP Quick Start Configuration Guide

Contents

Configuring an NTP client to synchronize the time with an NTP server ·········· 1

Introduction ·· 1
Network configuration ·· 1
Procedure ··· 1
Verifying the configuration ·· 2
Configuration files ··· 3
Related documentation ·· 3

Configuring an NTP client to synchronize the time with an NTP server

Introduction

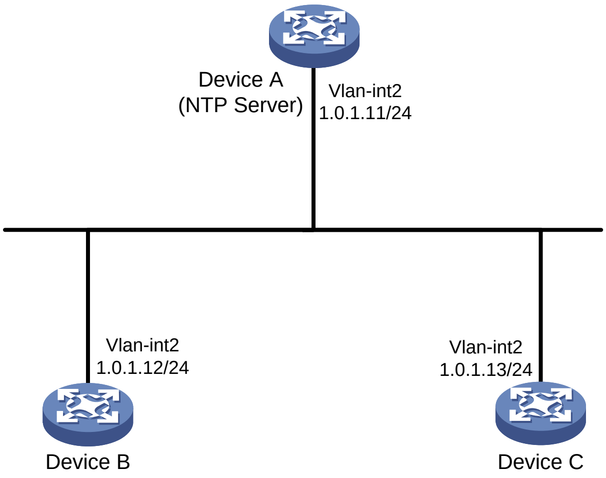
The following information uses an example to describe the basic procedure for configuring an NTP client to synchronize the time with an NTP server.

Network configuration

As shown in Figure 1, configure Device B and Device C to synchronize the time with Device A through NTP. To meet this requirement:

- On device A, specify the local clock as its reference source and set the stratum level of the clock to 2.
- Configure Device B to operate in NTP client mode and specify Device A as its NTP server.
- Configure Device C to operate in NTP client mode and specify Device A as its NTP server.

Figure 1 Network diagram



Procedure

1. Configure Device A.

   # Assign an interface 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 NTP.

```
[DeviceA] ntp-service enable
```

   # Specify the local clock as the reference source and set the stratum level of the clock to 2.

```
[DeviceA] ntp-service refclock-master 2
```

2. Configure Device B

   # Assign an interface to VLAN-interface 2.

   ```
   <DeviceB> system-view
   [DeviceB] interface Vlan-interface2
   [DeviceB-Vlan-interface2] ip address 1.0.1.12 24
   [DeviceB-Vlan-interface2] quit
   ```

   # Enable NTP.

   ```
   <DeviceB> system-view
   [DeviceB] ntp-service enable
   ```

   # Specify NTP for obtaining the time.

   ```
   [DeviceB] clock protocol ntp
   ```

   # Specify Device A as the NTP server.

   ```
   [DeviceB] ntp-service unicast-server 1.0.1.11
   ```

3. Configure Device C.

   # Assign an interface to VLAN-interface 2.

   ```
   <DeviceC> system-view
   [DeviceC] interface Vlan-interface2
   [DeviceC-Vlan-interface2] ip address 1.0.1.13 24
   [DeviceC-Vlan-interface2] quit
   ```

   # Enable NTP.

   ```
   <DeviceC> system-view
   [DeviceC] ntp-service enable
   ```

   # Specify NTP for obtaining the time.

   ```
   [DeviceC] clock protocol ntp
   ```

   # Specify Device A as the NTP server.

   ```
   [DeviceC] ntp-service unicast-server 1.0.1.11
   ```

Verifying the configuration

Verify that Device B and Device C have synchronized the time with Device C. The following uses Device B as an example to verify the configuration.

# Execute the **`display ntp-service status`** command on Device B to display its NTP status.

```
[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: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-10
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2019 18:58:07.724
 System poll interval: 64 s
```

The command output shows that Device B has synchronized its time with Device A, and the clock stratum level of Device B is 3.

# 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   15   -4.0 0.0038 16.262
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
     Total sessions: 1
```

Configuration files

- Device A:

```
#
 interface Vlan-interface2
 ip address 1.0.1.11 24
 quit
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B:

```
#
 interface Vlan-interface2
 ip address 1.0.1.12 24
 quit
 ntp-service enable
 clock protocol ntp
 ntp-service unicast-server 1.0.1.11
#
```

- Device C:

```
#
interface Vlan-interface2
 ip address 1.0.1.13 24
#
 ntp-service enable
 clock protocol ntp
 ntp-service unicast-server 1.0.1.11
#
```

Related documentation

- NTP configuration in the network management and monitoring configuration guide for the device.
- NTP commands in the network management and monitoring command reference for the device.

RBAC Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring RBAC for a local authentication user ··· 1

Introduction ··· 1
Network configuration ··· 1
Restrictions and guidelines ··· 1
Procedure ··· 1
Verifying the configuration ··· 2
Configuration files ··· 3
Related documentation ··· 4

Configuring RBAC temporary user role authorization ··· 5

Introduction ··· 5
Network configuration ··· 5
Restrictions and guidelines ··· 5
Procedure ··· 6
Verifying the configuration ··· 7
Configuration files ··· 10
Related documentation ··· 11

Configuring RBAC for a local authentication user

Introduction

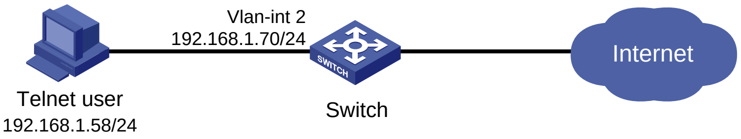
The following information uses an example to describe the basic procedure for configuring RBAC for a local authentication user.

Network configuration

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

- The switch performs local AAA authentication and authorization for the Telnet user.
- The user account for the Telnet user is **user1@bbb**, which is assigned user role **role1** with the following permissions:
  - Execute the read commands of any feature.
  - Access VLANs 10 to 20. Access to any other VLANs is denied.

Figure 1 Network diagram



Restrictions and guidelines

An ISP domain cannot be directly deleted when it is the default ISP domain. To delete the domain, you must first change it to a non-default ISP domain by using the **`undo domain default enable`** command.

You can configure user role rules to permit or deny the access of a user role to specific commands. If two rules conflict, the rule with the higher ID takes effect. For example, a user role can execute command B but not command A if the user role contains rules configured by using the following commands:

- **`rule`** *1* **`permit command`** *A*
- **`rule`** *2* **`permit command`** *B*
- **`rule`** *3* **`deny command`** *A*

Procedure

# Set the name of the switch to **Switch**.

```
<H3C> system-view
[H3C] sysname Switch
```

# Assign an IP address to VLAN-interface 2 (the interface connected to the Telnet user).

```
[Switch] interface vlan-interface 2
```

```
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

# Enable the Telnet server.

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

# Enable scheme authentication on the user lines for Telnet users.

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

# Enable local authentication and authorization for ISP domain **bbb**.

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

# Create a user role named **role1** and enter its view.

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

# Configure rule 1 to permit the user role to execute the read commands of all features.

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

# Configure rule 2 to permit the user role to create VLANs and access commands in VLAN view.

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

# Change the VLAN policy to permit the user role to configure only VLANs 10 to 20.

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

# Create a device management user named **user1** and enter local user view.

```
[Switch] local-user user1 class manage
```

# Set a plaintext password of **123456TESTplat&!** for the user.

```
[Switch-luser-manage-user1] password simple 123456TESTplat&!
```

# Set the service type to **Telnet**.

```
[Switch-luser-manage-user1] service-type telnet
```

# Assign **role1** to the user.

```
[Switch-luser-manage-user1] authorization-attribute user-role role1
```

# Remove the default user role (**network-operator**) in the user account. This operation ensures that the user has only the permissions of **role1**.

```
[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator
[Switch-luser-manage-user1] quit
```

Verifying the configuration

# Verify that you can successfully log in to the switch by entering username **user1@bbb** and password on the Telnet client.

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: user1@bbb
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.                     *
******************************************************************************

<Switch>
```

# Verify that you can log in as **role1** and execute the corresponding commands:

- Verify that you can create VLANs 10 to 20. This example uses VLAN 10.

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

- Verify that you cannot create any VLAN other than VLANs 10 to 20. This example uses VLAN 30.

  ```
  [Switch] vlan 30
  Permission denied.
  ```

- Verify that you can execute all read commands of any feature. This example uses the **display clock** command.

  ```
  [Switch] display clock
  09:31:56.258 UTC Sat 01/01/2017
  [Switch] quit
  ```

- Verify that you cannot execute the write or execute commands of any feature.

  ```
  <Switch> debugging role all
  Permission denied.
  <Switch> ping 192.168.1.58
  Permission denied.
  ```

Configuration files

```
#
 sysname Switch
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read feature
```

```
 rule 2 permit command system-view ; vlan *
 vlan policy deny
  permit vlan 10 to 20
#
local-user user1 class manage
 password hash $h$6$3nDcf1enrif2H0W6$QUWsXcld9MjeCMWGlkU6qleuV3WqFFEE8i2TTSoFRL3
ENZ2ExkhXZZrRmOl3pblfbje6fim7vV+u5FbCif+SjA==
 service-type telnet
 authorization-attribute user-role role1
 undo authorization-attribute user-role network-operator
#
```

Related documentation

- RBAC configuration in the fundamentals configuration guide for the device.
- RBAC commands in the fundamentals command reference for the device.

Configuring RBAC temporary user role authorization

Introduction

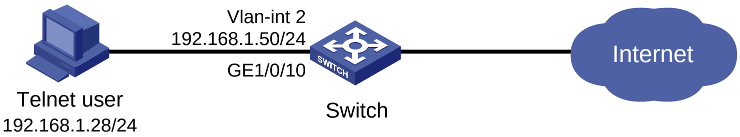
The following information uses an example to describe the basic procedure for configuring RBAC temporary user role authorization.

Network configuration

As shown in Figure 2, configure the switch to meet the following requirements:

- The switch performs local AAA authentication and authorization for the Telnet user.
- The user account for the Telnet user is **user1@bbb**, which is assigned user role **role1** with the following permissions:
    - Execute all Layer 3 feature commands in predefined feature group **L3**.
    - Execute all **`display`** commands.
    - Execute all **`super`** commands.
    - Access all interfaces, VLANs, and VPN instances.
- The user role of the Telnet user can be temporarily changed to **role2** or **network-operator** on the current login. User role **role2** has the following permissions:
    - Execute all Layer 2 feature commands in predefined feature group **L2**.
    - Access all interfaces, VLANs, and VPN instances.

Figure 2 Network diagram



Restrictions and guidelines

An ISP domain cannot be directly deleted when it is the default ISP domain. To delete the domain, you must first change the domain to a non-default ISP domain by using the **`undo domain default enable`** command.

You can configure user role rules to permit or deny the access of a user role to specific commands. If two rules conflict, the rule with the higher ID takes effect. For example, a user role can execute command B but not command A if the user role contains rules configured by using the following commands:

- **`rule`** *1* **`permit command`** *A*
- **`rule`** *2* **`permit command`** *B*
- **`rule`** *3* **`deny command`** *A*

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.

Procedure

# Set the name of the switch to **Switch**.

```
<H3C> system-view
[H3C] sysname Switch
```

# Create VLAN 2 and assign GigabitEthernet 1/0/10 (the port connected to the Telnet user) to VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface GigabitEthernet1/0/10
[Switch-GigabitEthernet1/0/10] port access vlan 2
[Switch-GigabitEthernet1/0/10] quit
```

# Create VLAN-interface 2 and assign an IP address to the interface.

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

# Enable the Telnet server.

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

# Enable the login authentication mode to **scheme** on user lines VTY 0 through VTY 63 for Telnet users.

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

# Enable local authentication and authorization for ISP domain **bbb**.

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

# Create a user role named **role1** and enter its view.

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

# Configure rule 1 to permit the user role to execute all Layer 3 feature commands in predefined feature group **L3**.

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

# Configure rule 2 to permit the user role to execute all **`display`** commands.

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

# Configure rule 3 to permit the user role to execute all **`super`** commands.

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

# Create a user role named **role2** and enter its view.

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

# Configure rule 1 to permit the user role to execute all Layer 2 feature commands in predefined feature group **L2**.

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

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

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

# Set a plaintext password of **aabbcc** for the user.

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

# Set the service type to **Telnet**.

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

# Assign **role1** to the user.

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

# Remove the default user role (**network-operator**) from the user. This operation ensures that the user has only the permissions of **role1**.

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

# Enable local authentication for temporary user role authorization. (The default authentication mode is local authentication.)

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

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

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

# Set the local authentication password to **987654TESTplat&!** for user role **network-admin**.

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

Verifying the configuration

1. Verify that you can execute the **`display role`** command to view user role information and execute the **`display role feature-group`** command to view feature group information.

   # 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_changep
                                     assword
  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 securi
                                     ty-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
```

# Display the feature information of feature groups **L2** and **L3**. (Details not shown.)

2. Verify that you can log in to the switch.

# Verify that you can Telnet to the switch, and enter username **telnetuser@bbb** and password to log in to the switch.

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

<Switch>
```

3. Verify that you have access to the following commands before temporary user role authorization:

   # Verify that you can execute all Layer 3 feature commands in predefined feature group **L3**. This example creates VPN instance **vpn1**.

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

   # Verify that you can execute all **display** commands. This example uses the **display clock** command.

   ```
   <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
   ```

4. Verify temporary user role authorization:

   # Verify that you can execute all **super** commands in user view. This example uses the **super** command to obtain 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 execute all Layer 2 feature commands in predefined feature group **L2**. This example creates VLAN 10.

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

   # Verify that you cannot execute commands not in predefined feature group **L2** with user role **role2**. This example uses the **super** command to obtain user role **network-operator**.

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

   # Verify that you cannot execute the **display** commands with user role **role2**. This example uses the **display clock** command.

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

   # Verify that you can execute all **super** commands after you log in to the switch again. This example uses the **super** command to obtain the user role **network-operator**.

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

```
******************************************************************************

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

The output shows that the configuration has taken effect.

Configuration files

```
#
 sysname Switch
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface GigabitEthernet1/0/10
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
#
```

Related documentation

- RBAC configuration in the fundamentals configuration guide for the device.
- RBAC commands in the fundamentals command reference for the device.

IRF Quick Start Configuration Guide

Contents

Setting up a two-member IRF fabric ···· 1

Introduction ···· 1
Network configuration ···· 1
Analysis and data preparation ···· 1
Restrictions and guidelines ···· 2
Procedures ···· 2
Verifying the configuration ···· 3
Configuration files ···· 4
Related documentation ···· 4

Configuring BFD MAD for IRF split detection ···· 5

Introduction ···· 5
Network configuration ···· 5
Restrictions and guidelines ···· 6
Procedures ···· 6
Verifying the configuration ···· 7
Configuration files ···· 8
Related documentation ···· 8

Setting up a two-member IRF fabric

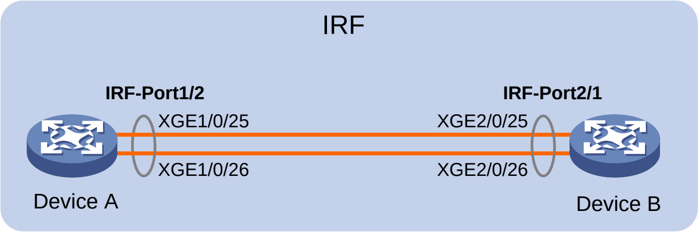
Introduction

The Intelligent Resilient Framework (IRF) technology enables you to add device nodes for forwarding capacity expansion without changing network topology. The following information uses an example to describe the basic procedure for two-member IRF fabric setup.

Network configuration

As shown in Figure 1, add Device B to expand Device A at the core layer of a network into a two-member IRF fabric to accommodate growing traffic without changing the network topology.

Figure 1 Network diagram



Analysis and data preparation

The following is the summary procedure for IRF setup:

1. Assign a unique IRF member ID to each device.

   If you change the IRF member ID of a device, you must reboot the device for the new member ID to take effect.
2. Assign an IRF member priority to each device for master election.

   Assign a higher priority to the device to be used as the master.
3. Bind physical interfaces to IRF ports.
4. Save the configuration.
5. Connect the peer IRF physical interfaces between the IRF member devices.
6. Activate the IRF port settings on each device.

This example uses the configuration data in Table 1 for IRF setup.

Table 1 Configuration data

Device	IRF member ID	IRF member priority	IRF port bindings
Device A	1 (default)	32	IRF port: irf-port 1/2 IRF physical interfaces: • Ten-GigabitEthernet 1/0/25 • Ten-GigabitEthernet 1/0/26

Device	IRF member ID	IRF member priority	IRF port bindings
Device B	2	1 (default)	IRF port: irf-port 2/1 IRF physical interfaces: • Ten-GigabitEthernet 2/0/25 • Ten-GigabitEthernet 2/0/26

Restrictions and guidelines

IRF ports are numbered in *member-id*/*port-id* format, with *port-id* being 1 or 2. To set up an IRF fabric, make sure the peer IRF ports connected between neighboring member devices have different port IDs. If you use IRF-port *member-id*/1 on one member device, you must connect it to IRF-port *member-id*/2 on the other.

For example, Device A has a member ID of 1 and Device B has a member ID of 2. You can use either of the following IRF port connection schemes:

- IRF-port 1/2 (Device A) to IRF-port 2/1 (Device B). This example uses this connection scheme.
- IRF-port 1/1 (Device A) to IRF-port 2/2 (Device B).

Procedures

Configuring Device A

# Assign a member ID to Device A. In this example, this step is skipped for Device A, because it uses the default member ID (1).

# Bind Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26 to IRF-port 1/2.

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] interface ten-gigabitethernet 1/0/26
[DeviceA-Ten-GigabitEthernet1/0/26] shutdown
[DeviceA-Ten-GigabitEthernet1/0/26] quit
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet1/0/25
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet1/0/26
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] interface ten-gigabitethernet 1/0/26
[DeviceA-Ten-GigabitEthernet1/0/26] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/26] quit
```

# Assign IRF member priority 32 to Device A. This priority is high enough to ensure that Device A can be elected as the master.

```
[DeviceA] irf member 1 priority 32
```

# Save the configuration.

```
[DeviceA] save force
```

Configuring Device B

# Assign member ID 2 to Device B, and then reboot the device to have the new member ID take effect.

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

# Bind Ten-GigabitEthernet 2/0/25 and Ten-GigabitEthernet 2/0/26 to IRF-port 2/1.

```
[DeviceB] interface ten-gigabitethernet 2/0/25
[DeviceB-Ten-GigabitEthernet2/0/25] shutdown
[DeviceB-Ten-GigabitEthernet2/0/25] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet2/0/25
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet2/0/26
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/0/25
[DeviceB-Ten-GigabitEthernet2/0/25] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/25] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] quit
```

# Save the configuration.

```
[DeviceB] save force
```

# Connect the IRF physical interfaces on Device B to their peer IRF physical interfaces on Device A, as shown in Figure 1.

Activating the IRF port settings

# Activate the IRF port settings on Device A.

```
[DeviceA] irf-port-configuration active
```

# Activate the IRF port settings on Device B.

```
[DeviceB] irf-port-configuration active
```

Device B and Device perform master election automatically. With a lower priority than Device A, Device B fails master election and reboots to form an IRF fabric with Device A. The system name of the IRF fabric is Device A.

Verifying the configuration

# Verify that the IRF fabric has been established.

```
<DeviceA> display irf
MemberID  Slot  Role    Priority  CPU-Mac         Description
 *+1      0     Master  32        0210-fc01-0000  ---
   2      0     Standby 1         0210-fc02-0000  ---
--------------------------------------------------
```

```
* indicates the device is the master.
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 3822-d60f-2800
Auto upgrade                : yes
Mac persistent              : always
Domain ID                   : 0
Auto merge                  : yes
```

The output shows that the IRF fabric has been established.

Configuration files

- Device A:

```
#
 irf member 1 renumber 2
#
irf-port 1/2
 port group interface ten-gigabitethernet1/0/25
 port group interface ten-gigabitethernet1/0/26
#
 irf-port-configuration active
#
```

- Device B:

```
#
irf-port 2/1
 port group interface ten-gigabitethernet2/0/25
 port group interface ten-gigabitethernet2/0/26
#
 irf-port-configuration active
#
```

Related documentation

- IRF configuration in the virtual technologies configuration guide for the device.
- IRF commands in the virtual technologies command reference for the device.

Configuring BFD MAD for IRF split detection

Introduction

IRF link failure might cause an IRF fabric to split in two IRF fabrics operating with the same Layer 3 settings, including the same IP address. To avoid IP address collision and other network issues caused by an IRF split, IRF provides multi-active detection (MAD) mechanisms to detect the presence of multiple conflicting active IRF fabrics, handle collisions, and recover from faults. One of the most commonly used MAD mechanisms extends the Bidirectional Forwarding Detection (BFD) protocol to detect multi-active conflicts.

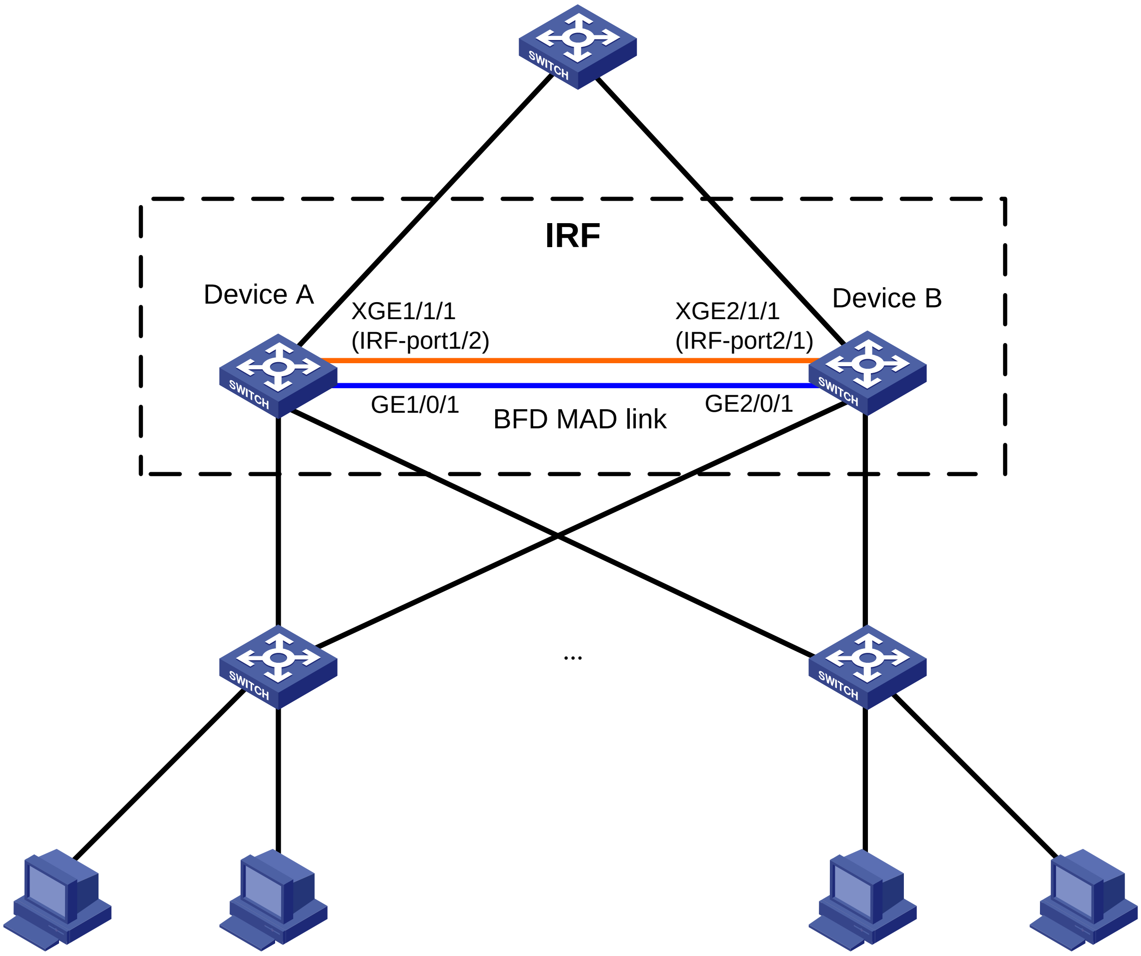
When a two-member IRF fabric splits, BFD MAD places the device with the higher member ID in Recovery state and shuts down all common network interfaces on it except for the interfaces automatically or manually excluded from being shut down by any MAD mechanisms. In this situation, only the device with the lower member ID can continue to forward traffic.

The following information uses an example to describe the basis BFD MAD configuration procedure.

Network configuration

Figure 2 shows an IRF fabric that contains Device A and Device B. Configure BFD MAD on the IRF fabric to detect multi-active conflicts.

Figure 2 Network diagram



Restrictions and guidelines

- Disable the spanning tree feature on all Layer 2 Ethernet ports in the BFD MAD VLAN. BFD MAD is mutually exclusive with the spanning tree feature.
- Do not configure the BFD MAD VLAN interface and its member ports for any purpose other than BFD MAD. If you configure them to provide other services, both BFD MAD and other services might operate incorrectly.

Procedures

Setting up the IRF fabric

Configure Device A and Device B to establish an IRF fabric. For more information about the procedure see "Setting up a two-member IRF fabric."

Configuring BFD MAD on the IRF fabric

# Create VLAN 3 (BFD MAD VLAN) and add port GigabitEthernet 1/0/1 on Device A and port GigabitEthernet 2/0/1 on Device B to the VLAN.

```
<IRF> system-view
[IRF] vlan 3
[IRF-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1
```

```
[IRF-vlan3] quit
```

# Create VLAN-interface 3 and assign a MAD IP address to each member device on the interface.

```
[IRF] interface vlan-interface 3
[IRF-Vlan-interface3] mad bfd enable
[IRF-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[IRF-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[IRF-Vlan-interface3] quit
```

# Disable the spanning tree feature on the ports in the BFD MAD VLAN.

```
[IRF] interface gigabitethernet 1/0/1
[IRF-gigabitethernet1/0/1] undo stp enable
[IRF-gigabitethernet1/0/1] quit
[IRF] interface gigabitethernet 2/0/1
[IRF-gigabitethernet2/0/1] undo stp enable
```

Verifying the configuration

After the IRF fabric splits, verify that BFD MAD operates correctly:

# Execute the **`display mad verbose`** command on Device A. Verify that the **Multi-active recovery state** field in the command output is **No** and Device A can continue to forward traffic.

```
<DeviceA> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled.
<DeviceA> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
Ten-GigabitEthernet1/1/1
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface3
  MAD status                 : Faulty
  Member ID   MAD IP address       Neighbor    MAD status
  1           192.168.2.1/24       2           Faulty
```

# On Device B, execute the **`display interface brief down`** command. Verify that all network ports on it have been shut down by MAD except those automatically or manually excluded from the MAD shutdown action.

```
<DeviceB> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface Link Cause
GE2/0/2 DOWN MAD ShutDown
GE2/0/3 DOWN MAD ShutDown
```

Configuration files

```
#
vlan 3
 port gigabitethernet 1/0/1 gigabitethernet 2/0/1
#
interface vlan-interface 3
 mad bfd enable
 mad ip address 192.168.2.1 24 member 1
 mad ip address 192.168.2.2 24 member 2
#
interface gigabitethernet 1/0/1
 undo stp enable
#
interface gigabitethernet 2/0/1
 undo stp enable
#
```

Related documentation

- IRF configuration in the virtual technologies configuration guide for the device.
- IRF commands in the virtual technologies command reference for the device.

Ethernet Interface Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Activating the copper port or fiber port of a combo interface ··························· 1

Introduction ······ 1
Network configuration ······ 1
Restrictions and guidelines ······ 1
Procedure······ 1
Verifying the configuration······ 1
Configuration files ······ 2
Related documentation ······ 2

Activating the copper port or fiber port of a combo interface

Introduction

The following information uses an example to describe the basic procedure for activating the copper port or fiber port of a combo interface.

Network configuration

Activate the copper port or fiber port of a combo interface at the CLI.

Restrictions and guidelines

A combo interface is a logical interface that physically comprises one fiber combo port and one copper combo port on the device panel. The two ports share one forwarding interface and one interface view. As a result, they cannot work simultaneously. When you activate one port, the other port is automatically disabled.

Procedure

# Activate the copper combo port of GigabitEthernet 1/0/1, and connect a twisted pair cable to the interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable copper
[Sysname-GigabitEthernet1/0/1] quit
```

# Activate the fiber combo port of GigabitEthernet 1/0/1, and connect a fiber to the interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable fiber
[Sysname-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# When a combo interface is connected to a cable or transceiver module, use the **`display interface`** command to view information about the interface. If **Media type is twisted pair** is displayed in the command output, the copper port is activated. If not, the fiber port is activated.

```
[Sysname] display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 00ff-00ff-0139
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
```

```
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
…
```

Configuration files

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable copper
#
```

Related documentation

- Ethernet interface configuration in the Layer 2—Ethernet switching configuration guide for the device.
- Ethernet interface commands in the Layer 2—Ethernet switching command reference for the device.

VLAN Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring port-based VLANs ··· 1

Introduction ··· 1
Network configuration ··· 1
Procedures ··· 1
Verifying the configuration ··· 2
Configuration files ··· 3
Related documentation ··· 4

Configuring super VLANs ··· 5

Introduction ··· 5
Network configuration ··· 5
Restrictions and guidelines ··· 5
Procedures ··· 5
Verifying the configuration ··· 7
Configuration files ··· 8
Related documentation ··· 9

Configuring voice VLANs ··· 10

Introduction ··· 10
Network configuration ··· 10
Procedures ··· 10
Verifying the configuration ··· 12
Configuration files ··· 12
Related documentation ··· 13

Configuring private VLAN ··· 14

Introduction ··· 14
Network configuration ··· 14
Restrictions and guidelines ··· 14
Procedures ··· 15
Verifying the configuration ··· 16
Configuration files ··· 17
Related documentation ··· 18

Configuring port-based VLANs

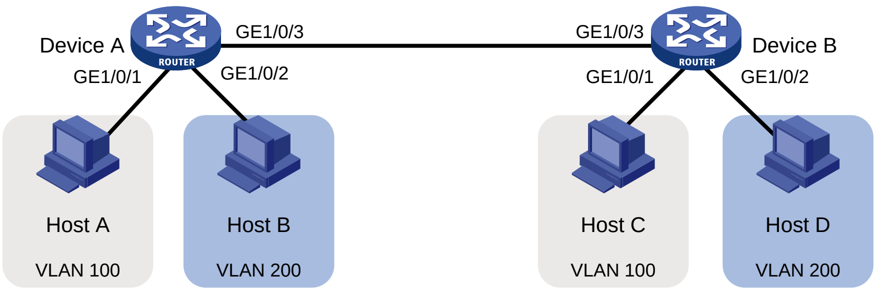
Introduction

The following information uses an example to describe the basic procedure for configuring port-based VLANs.

Network configuration

As shown in Figure 1, Host A and Host C belong to department A, but they access the company network through different devices. Host B and Host D belong to department B, but they access the company network through different devices. To ensure communication security and avoid flooding broadcast packets, you can use VLANs to isolate Layer 2 traffic of different departments. Configure department A to use VLAN 100, and configure department B to use VLAN 200. Then, hosts in the same VLAN can communicate. Host A and Host C can communicate. Host B and Host D can communicate.

Figure 1 Network diagram



Procedures

Configuring Device A

# Create VLAN 100. Assign GigabitEthernet 1/0/1 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

# Create VLAN 200. Assign GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceA] vlan 100
[DeviceA-vlan200] port GigabitEthernet 1/0/2
[DeviceA-vlan200] quit
```

# To forward packets from VLANs 100 and 200 on Device A to Device B, set the link type of GigabitEthernet 1/0/2 to trunk, 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
[DeviceA-GigabitEthernet1/0/3] quit
```

# Save the configuration.

```
[DeviceA] save force
```

Configuring Device B

# Create VLAN 100. Assign GigabitEthernet 1/0/1 to VLAN 100.

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitethernet 1/0/1
[DeviceB-vlan100] quit
```

# Create VLAN 200. Assign GigabitEthernet 1/0/2 to VLAN 200.

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitethernet 1/0/2
[DeviceB-vlan200] quit
```

# To forward packets from VLANs 100 and 200 on Device B to Device A, set the link type of GigabitEthernet 1/0/3 to trunk, and assign it to VLANs 100 and 200.

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/3] quit
```

# Save the configuration.

```
[DeviceB] save force
```

# Assign Host A and Host C to the same subnet, for example, 192.168.100.0/24. Assign Host B and Host D to the same subnet, for example, 192.168.200.0/24.

Verifying the configuration

# Display information about VLANs on Device A.

```
<DeviceA> display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/1(D)
<DeviceA> display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/2(D)
```

# Display information about VLANs on Device B.

```
<DeviceB> display vlan 100
```

```
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
GigabitEthernet1/0/1(D)
<DeviceB> display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/2(D)
```

Configuration files

- Device A:

```
#
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
```

- Device B:

```
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
```

Related documentation

- VLAN configuration in the Layer 2—Ethernet switching configuration guide for the device.
- VLAN commands in the Layer 2—Ethernet switching command reference for the device.

Configuring super VLANs

Introduction

The following information uses an example to describe the basic procedure for configuring super VLANs.

Network configuration

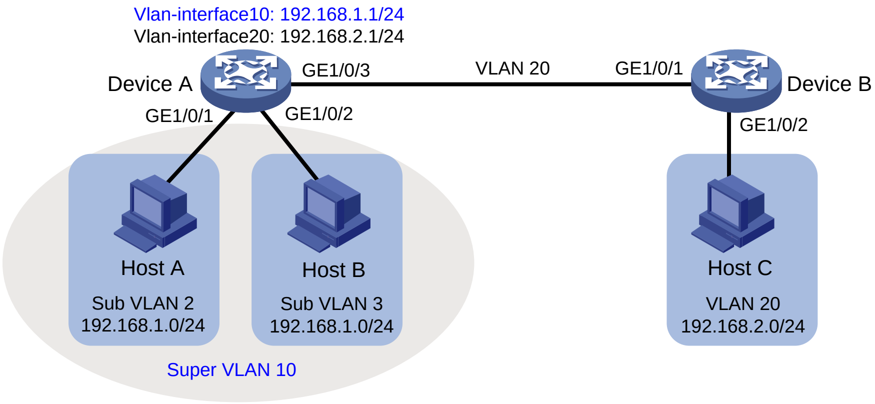
As shown in Figure 2:

- Users in VLAN 2 access the network through GigabitEthernet 1/0/1 on Device A. Users in VLAN 3 access the network through GigabitEthernet 1/0/2 on Device A. There are 30 users in VLAN 2 and 50 users in VLAN 3.
- GigabitEthernet 1/0/3 on Device A and GigabitEthernet 1/0/1 on Device B belong to VLAN 20.
- Endpoint users in VLAN 20 use the 192.168.2.0/24 subnet and use 192.168.2.1 as the gateway address.

Configure a super VLAN to meet the following requirements:

- Endpoint users in VLAN 2 and VLAN 3 use the 192.168.1.0/24 subnet to save IP address resources and use 192.168.1.1 as the gateway address.
- Endpoints users in VLANs 2, 3, and 20 are isolated at Layer 2 and can communicate at Layer 3.

Figure 2 Network diagram



Restrictions and guidelines

A super VLAN cannot contain physical interfaces. If a VLAN already contains physical interfaces, you cannot configure it as a super VLAN.

Procedures

Configuring Device A

# Create VLAN 10, and configure it as a super VLAN.

```
<DeviceA> system-view
```

```
[DeviceA] vlan 100
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] quit
```

# Create VLAN 2. Assign GigabitEthernet 1/0/1 to VLAN 2.

```
[DeviceA] vlan 100
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

# Create VLAN 3. Assign GigabitEthernet 1/0/2 to VLAN 3.

```
[DeviceA] vlan 100
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
```

# Associate super VLAN 20 with sub-VLANs 2 and 3.

```
[DeviceA] vlan 100
[DeviceA-vlan10] subvlan 2 3
[DeviceA-vlan10] quit
```

# Assign an IP address to the VLAN interface for super VLAN 10, and enable local proxy on the VLAN interface.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

# Create VLAN 20.

```
[DeviceA] vlan 100
[DeviceA-vlan20] quit
```

# Set the link type of GigabitEthernet 1/0/3 to trunk and assign it to VLAN 20. Remove it 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
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20
[DeviceA-GigabitEthernet1/0/3] quit
```

# Assign an IP address to the VLAN interface for VLAN 20 .

```
[DeviceA] interface Vlan-interface 20
[DeviceA-Vlan-interface20] ip address 192.168.2.1 24
[DeviceA-Vlan-interface20] quit
```

# Save the configuration.

```
[DeviceA] save force
```

Configuring Device B

# Create VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk and assign it to VLAN 20. Remove it 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
```

```
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20
[DeviceB-GigabitEthernet1/0/1] quit
```

# Assign GigabitEthernet 1/0/2 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

# Save the configuration.

```
[DeviceB] save force
```

Verifying the configuration

# Display information about super VLANs on Device A.

```
<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
```

# Display information about VLAN 20 on Device A.

```
<DeviceA> display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports: None
```

# Display information about VLAN 20 on Device B.

```
<DeviceA> display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:
    GigabitEthernet1/0/2
```

Configuration files

- 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
#
```

Related documentation

- Super VLAN configuration in the Layer 2—Ethernet switching configuration guide for the device.
- Super VLAN commands in the Layer 2—Ethernet switching command reference for the device.

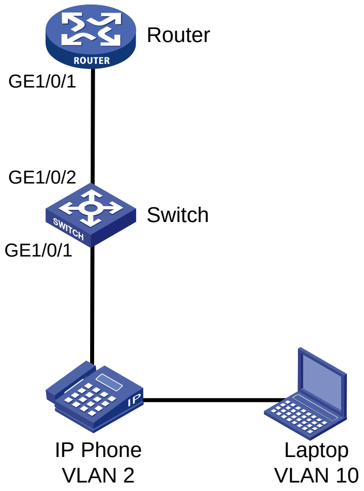
Configuring voice VLANs

Introduction

The following information uses an example to describe the basic procedure for configuring voice VLANs.

Network configuration

To ensure that voice traffic can be preferentially forwarded, you must separate the addresses of IP phones from those of laptops. Assign the subnet 192.168.2.0 to IP phones and assign the IP phones to VLAN 2. Assign the subnet 192.168.10.0 to laptops and assign the laptops to VLAN 10. Router acts as a DHCP server to allocate IP addresses to IP phones and laptops.



Procedures

Configuring Switch

# Enable PoE to supply power to phones.

```
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] poe enable
[Switch-GigabitEthernet1/0/1] quit
```

# Create VLAN 2 for phones and VLAN 10 for laptops.

```
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] vlan 10
[Switch-vlan10] quit
```

# Configure MAC addresses with prefix 6ca8-4900-0000 for voice packet identification.

```
[Switch] voice-vlan mac-address 6ca8-4900-0000 mask ffff-ff00-0000 description avaya
```

# Configure GigabitEthernet 1/0/1 as a hybrid port, and enable the voice VLAN feature on it.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] voice-vlan 2 enable
```

# Configure VLAN 10, to which laptops belong.

```
[Switch-GigabitEthernet1/0/1] port hybrid pvid vlan 10
[Switch-GigabitEthernet1/0/1] port hybrid vlan 10 untagged
[SWITCH-GigabitEthernet1/0/1] quit
```

# Assign interface GigabitEthernet 1/0/2 (which connects to the DHCP server) to VLANs 2 and 10.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 2 10
[Switch-GigabitEthernet1/0/2] quit
```

# Save the configuration.

```
[Switch] save force
```

Configuring Router

# Create VLAN 2 and VLAN10, and their VLAN interfaces. Assign IP addresses to the VLAN interfaces.

```
<Router> system-view
[Router] vlan 2
[Router-vlan2] quit
[Router] vlan 10
[Router-vlan10] quit
[Router] interface Vlan-interface 2
[Router-Vlan-interface2] ip address 192.168.2.1 255.255.255.0
[Router-Vlan-interface2] quit
[Router] interface Vlan-interface 10
[Router-Vlan-interface10] ip address 192.168.10.1 255.255.255.0
[Router-Vlan-interface10] quit
```

# Assign interface GigabitEthernet 1/0/1 (which connects to Switch) to VLANs 2 and 10.

```
[Router] interface GigabitEthernet 1/0/1
[Router-GigabitEthernet1/0/1] port link-type trunk
[Router-GigabitEthernet1/0/1] port trunk permit vlan 2 10
[Router-GigabitEthernet1/0/1] quit
```

# Enable the DHCP service.

```
[Router] dhcp enable
```

# Configure the DHCP address pool for VLAN 2, which contains phones.

```
[Router] dhcp server ip-pool vlan2
[Router-dhcp-pool-vlan2] network 192.168.2.0 mask 255.255.255.0
[Router-dhcp-pool-vlan2] gateway-list 192.168.2.1
[Router-dhcp-pool-vlan2] quit
```

# Configure the DHCP address pool for VLAN 10, which contains laptops.

```
[Router] dhcp server ip-pool vlan10
[Router-dhcp-pool-vlan10] network 192.168.10.0 mask 255.255.255.0
[Router-dhcp-pool-vlan10] gateway-list 192.168.10.1
[Router-dhcp-pool-vlan10] dns-list 114.114.114.114
[Router-dhcp-pool-vlan10] quit
```

# Save the configuration.

```
[Router] save force
```

Verifying the configuration

# On Switch, verify that phones are assigned to VLAN 2.

```
<Switch> display mac-address
MAC Address VLAN ID STATE Port/Nickname AGING
3897-d630-676b 10 Learned GE1/0/2 Y
3897-d630-676b 2 Learned GE1/0/2 Y
6ca8-4986-6d59 2 Learned GE1/0/1 Y
0068-eb95-3683 10 Learned GE1/0/1 Y
```

# Verify that the voice VLAN configuration takes effect.

```
<Switch> display voice-vlan mac-address
Oui Address Mask Description
0003-6b00-0000 ffff-ff00-0000 Cisco phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
6ca8-4900-0000 ffff-ff00-0000 avaya
```

# Verify that the voice VLAN assignment mode is auto.

```
<Switch> display voice-vlan state
Current Voice VLANs: 1
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT VLAN MODE COS DSCP
--------------------------------------------------------------------
GE1/0/1 2 AUTO 6 46
```

# On the DHCP server, view the IP addresses assigned to phones and laptops.

```
%Sep 1 09:19:59:333 2021 DHCP DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server information: Server
IP = 192.168.2.1, DHCP client IP = 192.168.2.2, DHCP client hardware address =
6ca8-4986-6d59, DHCP client lease = 86400.
<Router> display dhcp server ip-in-use all
Pool utilization: 0.59%
IP address Client-identifier/ Lease expiration Type
Hardware address
192.168.2.2 6ca8-4986-6d59 Aug 31 2021 09:19:59 Auto:COMMITTED
192.168.10.4 0068-eb95-3683 Aug 31 2021 09:19:42 Auto:COMMITTED
```

Configuration files

- Switch:

```
#
 voice-vlan mac-address 6ca8-4900-0000 mask ffff-ff00-0000 description avaya
#
vlan 2
#
vlan 10
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 10 untagged
 port hybrid pvid vlan 10
 voice-vlan 2 enable
 poe enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 10
```

- Router:

```
#
vlan 2
#
vlan 10
#
dhcp server ip-pool vlan2
 gateway-list 192.168.2.1
 network 192.168.2.0 255.255.255.0
#
dhcp server ip-pool vlan10
 gateway-list 192.168.10.1
 network 192.168.10.0 255.255.255.0
 dns-list 114.114.114.114
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 10
```

Related documentation

- Voice VLAN configuration in the Layer 2—Ethernet switching configuration guide for the device.
- Voice VLAN commands in the Layer 2—Ethernet switching command reference for the device.

Configuring private VLAN

Introduction

The following information uses an example to describe the basic procedure for configuring private VLAN.

Network configuration

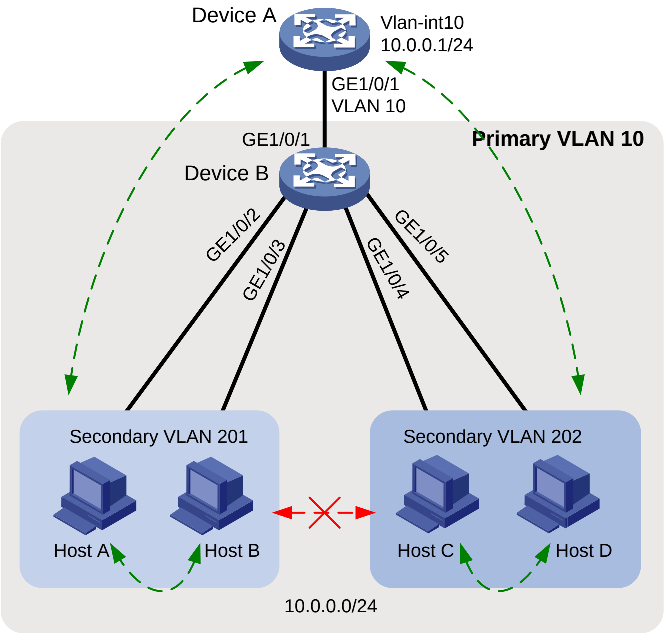
As shown in Figure 3:

- Device A on the aggregation layer assigns VLAN 10 to Device B on the access layer. The gateway interface (VLAN-interface 10) can communicate with all users, so that users can access Internet through Device A. All users attached to Device B are on the subnet 10.0.0.0/24.
- Hosts A and B belong to the sales department. Hosts C and D belong to the financial department. To ensure security, isolate different departments at Layer 2, and allow users in the same department to communicate with each other.

Because Device A cannot allocate more VLANs to Device B, configure the private VLAN feature to meet the following requirements:

- Device A only needs to recognize VLAN 10.
- In primary VLAN 10, Device B allocates different secondary VLANs to different departments, so these departments are isolated at Layer 2.

Figure 3 Network diagram



Restrictions and guidelines

- Configure the private VLAN feature only on the access device, Device B.
- The system default VLAN (VLAN 1) does not support private VLAN settings.

Procedures

Configuring Device B

# Configure VLAN 10 as the primary VLAN.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

# Create secondary VLANs 201 and 202.

```
[DeviceB] vlan 201 to 202
```

# Associate secondary VLANs 201 and 202 with the primary VLAN 10.

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 201 to 202
[DeviceB-vlan10] quit
```

# Configure the uplink port GigabitEthernet 1/0/1 to operate in promiscuous mode in 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, and assign GigabitEthernet 1/0/4 and GigabitEthernet 1/0/5 to VLAN 202. Configure them to operate in host mode.

```
[DeviceB] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[DeviceB-if-range] port access vlan 201
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
[DeviceB] interface range gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[DeviceB-if-range] port access vlan 202
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
```

# Save the configuration.

```
[DeviceB] save force
```

Configuring Device A

# Create VLAN 10. Assign GigabitEthernet 1/0/1 to VLAN 10.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan10] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

# Configure VLAN-interface 10, which is to act as the gateway.

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.0.0.1 24
[DeviceA-Vlan-interface10] quit
```

# Save the configuration.

```
[DeviceA] save force
```

Verifying the configuration

# Verify that you can ping any user from Device A. View the ARP table to verify that all users belong to VLAN 10.

```
[DeviceA] 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
10.0.0.2        0e9e-0671-0302 10            GE1/0/1                  1062  D
10.0.0.3        0e9e-09f7-0402 10            GE1/0/1                  1052  D
10.0.0.4        0e9e-0d94-0502 10            GE1/0/1                  1164  D
10.0.0.5        0e9e-1263-0602 10            GE1/0/1                  1109  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(U)            GigabitEthernet1/0/2(U)
    GigabitEthernet1/0/3(U)            GigabitEthernet1/0/4(U)
    GigabitEthernet1/0/5(U)

 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(U)            GigabitEthernet1/0/2(U)
    GigabitEthernet1/0/3(U)

 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(U)            GigabitEthernet1/0/4(U)
    GigabitEthernet1/0/5(U)
```

The output shows that GigabitEthernet 1/0/1 in promiscuous mode and GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 in host mode all allow packets to pass through untagged.

# Verify that Host A and Host B can ping each other, and Host C and Host D can ping each other. Verify that Host A or B cannot ping Host C or D.

Configuration files

- Device A:

```
#
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
#
```

- Device B:

```
#
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
#
```

Related documentation

- Private VLAN configuration in the Layer 2—Ethernet switching configuration guide for the device.
- Private VLAN commands in the Layer 2—Ethernet switching command reference for the device.

Port Isolation Quick Start Configuration Guide

Contents

Configuring port isolation ··· 1

Introduction ··· 1

Network configuration ··· 1

Restrictions and guidelines ··· 1

Procedure ··· 1

Verifying the configuration ··· 2

Configuration files ··· 2

Related documentation ··· 3

Configuring port isolation

Introduction

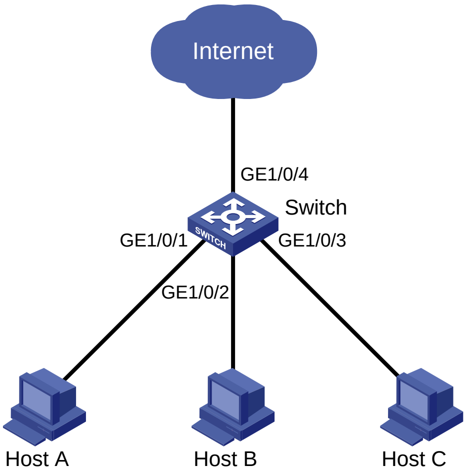
The following information uses an example to describe the basic port isolation configuration procedure.

Network configuration

As shown in Figure 1, the community users Host A, Host B, and Host C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of Switch, respectively. Switch is connected to Internet through GigabitEthernet 1/0/4.

Configure port isolation to isolate Layer 2 packets among Host A, Host B, and Host C, and allow these hosts to communicate with Internet.

Figure 1 Network diagram



Restrictions and guidelines

- To assign a port on a device to an isolation group, first create the isolation group.
- A port can be assigned to only one isolation group.

Procedure

IMPORTANT:

On a device that supports only one isolation group, the system automatically creates isolation group 1. You cannot delete the isolation group or create any other isolation group. On a device that supports multiple isolation groups, you can manually configure isolation groups.

# Create isolation group 1.

```
<Switch> system-view
[Switch] port-isolate group 1
```

# Assign ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to isolation group 1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-isolate enable group 1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port-isolate enable group 1
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port-isolate enable group 1
[Switch-GigabitEthernet1/0/3] quit
```

# Save the configuration.

```
[Switch] save force
```

Verifying the configuration

# Display information about isolation group 1.

```
[Switch] display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
```

The command output shows that GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on Switch have been assigned to isolation group 1 and isolated from each other at Layer 2. Host A, Host B, and Host C cannot ping each other.

Configuration files

```
#
 port-isolate group 1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-isolate enable group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port-isolate enable group 1
#
interface GigabitEthernet1/0/3
port link-mode bridge
port-isolate enable group 1
#
```

Related documentation

- Port isolation configuration in the Layer 2—Ethernet switching configuration guide for the device.
- Port isolation commands in the Layer 2—Ethernet switching command reference for the device.

Loop Detection Quick Start Configuration Guide

Contents

Configuring loop detection 1

Introduction 1

Network configuration 1

Procedure 1

Verifying the configuration 3

Configuration files 4

Related documentation 5

Configuring loop detection

Introduction

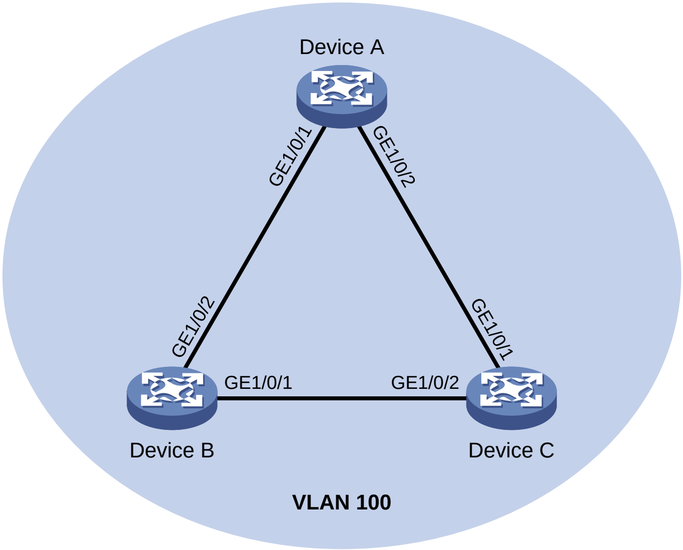
The following information uses an example to describe the basic procedure for configuring loop detection.

Network configuration

As shown in Figure 1, configure loop detection on Device A to meet the following requirements:

- Device A generates a log as a notification.
- Device A automatically shuts down the port on which a loop is detected.

Figure 1 Network diagram



Procedure

Configuring Device A

# Create VLAN 100, and globally enable loop detection for the VLAN.

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA–vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

# Set the global loop protection action to shutdown.

```
[DeviceA] loopback-detection global action shutdown
```

# Set the loop detection interval to 35 seconds.

```
[DeviceA] loopback-detection interval-time 35
```

# Save the configuration.

```
[DeviceA] save force
```

Configuring 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 them to VLAN 100.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[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 100
[DeviceB-GigabitEthernet1/0/2] quit
```

# Save the configuration.

```
[DeviceB] save force
```

Configuring Device C

# Create VLAN 100.

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

# Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports, and assign them to VLAN 100.

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[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 100
[DeviceC-GigabitEthernet1/0/2] quit
```

# Save the configuration.

```
[DeviceC] save force
```

Verifying the configuration

Verify the loop detection configuration on the devices. The following information uses Device A as an example.

# View the system logs.

```
<DeviceA> %Aug 26 19:17:29:760 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state
on the interface GigabitEthernet1/0/2 changed to up.
%Aug 26 19:17:29:760 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the
interface GigabitEthernet1/0/2 changed to up.
%Aug 26 19:17:30:356 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the
interface GigabitEthernet1/0/1 changed to up.
%Aug 26 19:17:30:356 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the
interface GigabitEthernet1/0/1 changed to up.
%Aug 26 19:17:33:985 2021 DeviceA LPDT/4/LPDT_LOOPED: -MDC=1; A loop was detected on
GigabitEthernet1/0/1.
%Aug 26 19:17:34:005 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the
interface GigabitEthernet1/0/1 changed to down.
%Aug 26 19:17:34:006 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the
interface GigabitEthernet1/0/1 changed to down.
%Aug 26 19:17:34:018 2021 DeviceA LPDT/4/LPDT_VLAN_LOOPED: -MDC=1; A loop was detected
on GigabitEthernet1/0/1 in VLAN 100.
%Aug 26 19:17:34:019 2021 DeviceA LPDT/4/LPDT_LOOPED: -MDC=1; A loop was detected on
GigabitEthernet1/0/2.
%Aug 26 19:17:34:040 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the
interface GigabitEthernet1/0/2 changed to down.
%Aug 26 19:17:34:041 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the
interface GigabitEthernet1/0/2 changed to down.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/4/LPDT_VLAN_LOOPED: -MDC=1; A loop was detected
on GigabitEthernet1/0/2 in VLAN 100.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: -MDC=1; A loop was removed
on GigabitEthernet1/0/1 in VLAN 100.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/5/LPDT_RECOVERED: -MDC=1; All loops were removed
on GigabitEthernet1/0/1.
%Aug 26 19:17:34:056 2021 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: -MDC=1; A loop was removed
on GigabitEthernet1/0/2 in VLAN 100.
%Aug 26 19:17:34:056 2021 DeviceA LPDT/5/LPDT_RECOVERED: -MDC=1; All loops were removed
on GigabitEthernet1/0/2.
```

The output shows the following information:

- Device A detected loops on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 within a loop detection interval.
- Loops on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 were removed.

# Use the **display loopback-detection** command to display the loop detection configuration and status.

```
<DeviceA> display loopback-detection
Loop detection is enabled.
Global loop detection interval is 35 second(s).
Loop is detected on following interfaces:
  Interface                        Action mode     VLANs/VSI
  GigabitEthernet1/0/1             Shutdown        100
  GigabitEthernet1/0/2             Shutdown        100
```

The output shows that the device has removed the loops from GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 according to the shutdown action.

# Display the status of GigabitEthernet 1/0/1.

```
<DeviceA> display interface gigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN (Loopback detection down)
```

The output shows that GigabitEthernet 1/0/1 is already shut down by the loop detection module.

# Display the status of GigabitEthernet 1/0/2.

```
<DeviceA>display interface gigabitEthernet 1/0/2
GigabitEthernet1/0/2
Current state: DOWN (Loopback detection down)
```

The output shows that GigabitEthernet 1/0/2 is already shut down by the loop detection module.

Configuration files

- Device A:

```
#
 loopback-detection global enable vlan 100
 loopback-detection global action shutdown
 loopback-detection interval-time 35
#
vlan 100
#
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 B:

```
#
vlan 100
#
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:

```
#
vlan 100
#
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
#
```

Related documentation

- Loop detection configuration in the Layer 2—LAN switching configuration guide for the device.
- Loop detection commands in the Layer 2—LAN switching command reference for the device.

QinQ Quick Start Configuration Guide

Content

Configuring basic QinQ 1

Introduction 1

Network configuration 1

Restrictions and guidelines 1

Procedure 1

Configuring CE 1 1

Configuring CE 2 2

Configuring PE A 2

Configuring PE B 3

Verifying the configuration 3

Configuration files 3

Related Documents 5

Configuring basic QinQ

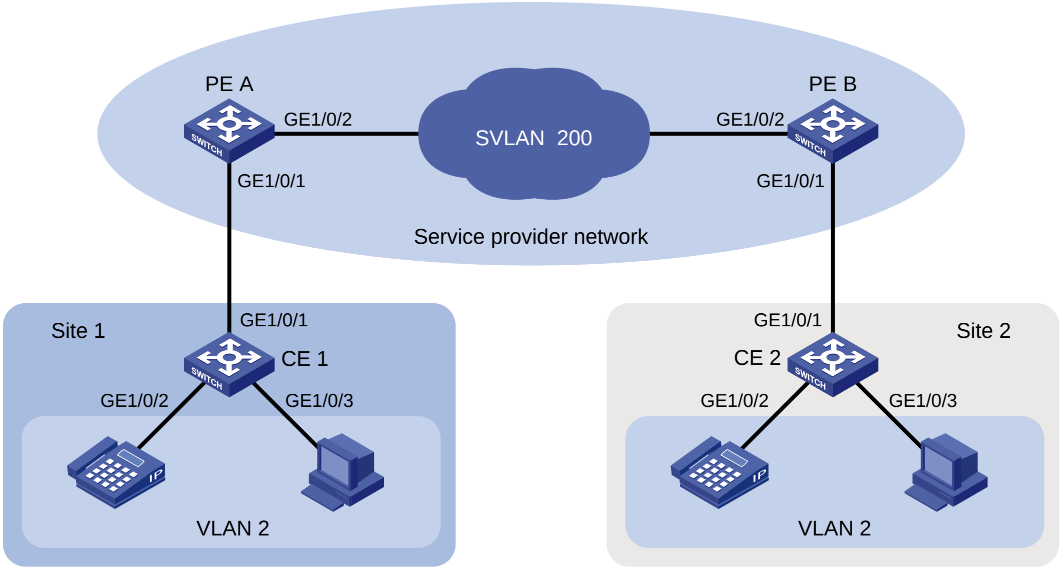
Introduction

The following information uses an example to describe the basic QinQ configuration procedure.

Network configuration

As shown in Figure 1, Site 1 and Site 2 belong to the same company and access the service provider network through access switches CE 1 and CE 2. VLAN 2 is used for internal network services of the company, and VLAN 200 is used in the service provider network. Configure QinQ on PE A and PE B to transmit traffic between Site 1 and Site 2 over the service provider network.

Figure 1 Network diagram



Restrictions and guidelines

Before enabling QinQ on a port, specify the PVID tag as the SVLAN tag for packet encapsulation.

Procedure

Configuring CE 1

# Create VLAN 2.

```
<CE 1> system-view
[CE 1] vlan 2
[CE 1-vlan2] quit
```

# Specify GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as access ports to allow packets from VLAN 2 to pass through.

```
[CE 1] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[CE 1-if-range] port access vlan 2
[CE 1-if-range] quit
```

# Specify GigabitEthernet 1/0/1 as a trunk port to allow packets from VLAN 2 to pass through.

```
[CE 1] interface gigabitethernet 1/0/1
[CE 1-GigabitEthernet1/0/1] port link-type trunk
[CE 1-GigabitEthernet1/0/1] port trunk permit vlan 2
[CE 1-GigabitEthernet1/0/1] quit
```

Configuring CE 2

Configure CE 2 in the same way CE 1 is configured. (Details not shown.)

Configuring PE A

# Create VLAN 2 and VLAN 200.

```
<PE A> system-view
[PE A] vlan 2
[PE A-vlan2] quit
[PE A] vlan 200
[PE A-vlan200] quit
```

# Specify GigabitEthernet 1/0/1 as a trunk port to allow packets from VLAN 2 and VLAN 200 to pass through.

```
[PE A] interface gigabitethernet 1/0/1
[PE A-GigabitEthernet1/0/1] port link-type trunk
[PE A-GigabitEthernet1/0/1] port trunk permit vlan 2 200
```

# Specify the PVID as VLAN 200 for GigabitEthernet 1/0/1.

```
[PE A-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

# Enable QinQ for GigabitEthernet 1/0/1.

```
[PE A-GigabitEthernet1/0/1] qinq enable
[PE A-GigabitEthernet1/0/1] quit
```

# Specify GigabitEthernet 1/0/2 as a trunk port to allow packets from VLAN 200 to pass through.

```
[PE A] interface gigabitethernet 1/0/2
[PE A-GigabitEthernet1/0/2] port link-type trunk
[PE A-GigabitEthernet1/0/2] port trunk permit vlan 200
[PE A-GigabitEthernet1/0/2] quit
```

Configuring PE B

Configure PE B in the same way PE A is configured. (Details not shown.)

Verifying the configuration

Verify that a PC at Site 1 and a PC at Site 2 can ping each other successfully and learn the MAC addresses from each other. CVLAN information can be transparently transmited between the two PCs over the service provider network.

# Ping a PC at Site 2 from a PC at Site 1 to verify the connectivity.

```
C:\Users\usera>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=28ms TTL=253
Reply from 192.168.1.2: bytes =32 time =27ms TTL=253
Reply from 192.168.1.2: bytes =32 time =27ms TTL=253
Reply from 192.168.1.2: bytes =32 time =26ms TTL=253

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% Loss),
Approximate round trip time in milli-seconds:
    Minimum = 26ms, Maximum = 28ms, Average = 27ms
```

# View the MAC address table on CE 1 to verify that CE 1 has learned the MAC address of the PC at Site 2.

```
<Sysname> display mac-address vlan 2
MAC Address      VLAN ID    State            Port/Nickname            Aging
0003-2d00-5761   2          Learned          GE1/0/1                  Y
```

Configuration files

- CE 1

```
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port access vlan 2
```

- CE 2

```
#
vlan 2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
#
interface GigabitEthernet1/0/3
 port access vlan 2
```

- PE A

```
#
vlan 2
#
Vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2 200
 port trunk pvid vlan 200
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 200
```

- PE B

```
#
vlan 2
#
Vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2 200
 port trunk pvid vlan 200
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 200
#
```

Related Documents

- QinQ configuration in the Layer 2—LAN switching configuration guide for the device.
- QinQ commands in the Layer 2—LAN switching command reference for the device.

MAC Address Table Quick Start Configuration Guide

Contents

Configuring static MAC address entries 1

Introduction 1

Network configuration 1

Procedure 1

Verifying the configuration 2

Configuration files 2

Related documentation 2

Configuring static MAC address entries

Introduction

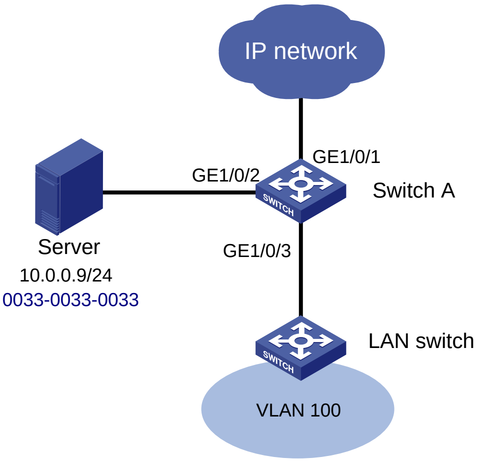
The following information uses an example to describe the basic procedure for configuring static MAC address entries.

Network configuration

As shown in Figure 1, for secure communication between users in VLAN 100 and the server or extranet through Switch A, perform the following tasks:

- Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 100.
- Add a static MAC address entry on Switch A to bind the server MAC address to GigabitEthernet 1/0/2.

Figure 1 Network diagram



Procedure

To Configure Switch A:

# Create VLAN 100.

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] quit
```

# Assign GigabitEthernet 1/0/2 to VLAN 100.

```
[Switch A] interface gigabitethernet 1/0/2
[Switch A-GigabitEthernet1/0/2] port access vlan 100
[Switch A-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 (port facing the LAN switch) as a trunk port, and assign the port to VLAN 100.

```
[Switch A] interface gigabitethernet 1/0/3
[Switch A-GigabitEthernet1/0/3] port link-type trunk
```

```
[Switch A-GigabitEthernet1/0/3] port trunk permit vlan 100
[Switch A-GigabitEthernet1/0/3] quit
```

# Add a static entry for MAC address 0033-0033-0033 on GigabitEthernet 1/0/2 that belongs to VLAN 100.

```
[Switch A] mac-address static 0033-0033-0033 interface gigabitethernet 1/0/2 vlan 100
```

Verifying the configuration

# Use ping operations to verify that any 10.0.0.0/24 host in VLAN 100 can communicate with the server.

```
<Sysname> ping 10.0.0.9
Ping 10.0.0.9 (10.0.0.9): 56 data bytes, press CTRL+C to break
56 bytes from 10.0.0.9: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 10.0.0.9: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.0.0.9: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.0.0.9: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.0.0.9: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 10.0.0.9 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

# Verify that the static MAC address entry has been added.

```
[Switch A] display mac-address
MAC Address      VLAN ID    State            Port/NickName            Aging
0033-0033-0033   100        Static           GE1/0/2                  N
```

Configuration files

```
#
vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 mac-address static 0033-0033-0033 vlan 100
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100
#
```

Related documentation

- MAC address table configuration in the Layer 2—LAN switching configuration guide for the device.
- MAC address table commands in the Layer 2—LAN switching command reference for the device.

Ethernet Link Aggregation Quick Start Configuration Guide

Contents

Configuring Layer 2 link aggregation ··· 1

Introduction ··· 1

Network configuration ··· 1

Restrictions and guidelines ··· 1

Procedure··· 2

Verifying the configuration··· 3

Configuration files ··· 4

Related documentation ··· 5

Configuring Layer 2 link aggregation

Introduction

The following information uses an example to describe the basic procedure for configuring Layer 2 link aggregation.

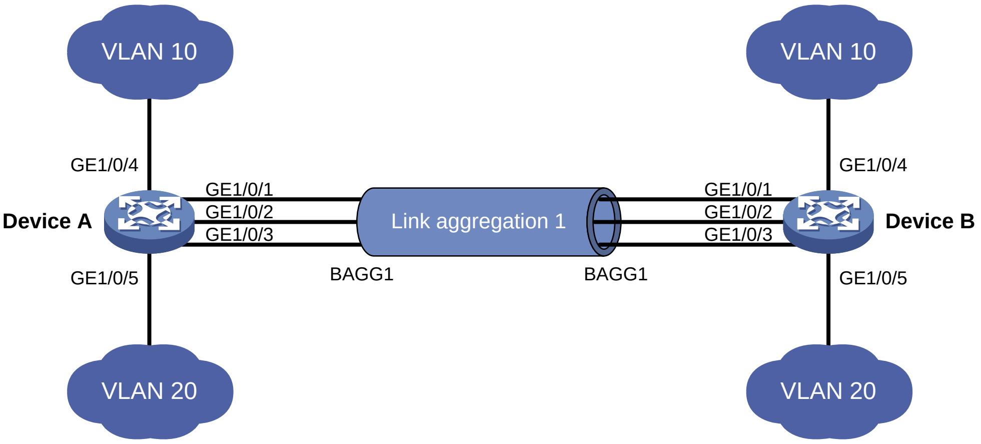
Network configuration

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



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.

Procedure

Configuring Device A

# Enter system view, create VLAN 10, and then 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 static or dynamic Layer 2 aggregate interface Bridge-aggregation 1.

- Create static Layer 2 aggregate interface Bridge-aggregation 1.

  ```
  [DeviceA] interface bridge-aggregation 1
  [DeviceA-Bridge-Aggregation1] 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] undo shutdown
  [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] undo shutdown
[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
```

Configuring Device B

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.

- Display link aggregation configuration 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.

- Display link aggregation configuration 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    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    1        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/2             32768    2        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/3             32768    3        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 aggregation state through exchanging LACPDUs.

Configuration files

- 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.

Related documentation

- Ethernet link aggregation configuration in the Layer 2—LAN switching configuration guide for the device.
- Ethernet link aggregation commands in the Layer 2—LAN switching command reference for the device.

Spanning Tree Quick Start Configuration Guide

Contents

Configuring MSTP ··· 1

Introduction ··· 1
Network configuration ··· 1
Analysis ··· 1
Procedure ··· 2
Verifying the configuration ··· 4
Configuration files ··· 7
Related documentation ··· 9

Configuring MSTP

Introduction

The following information uses an example to describe the basic procedure for configuring MSTP.

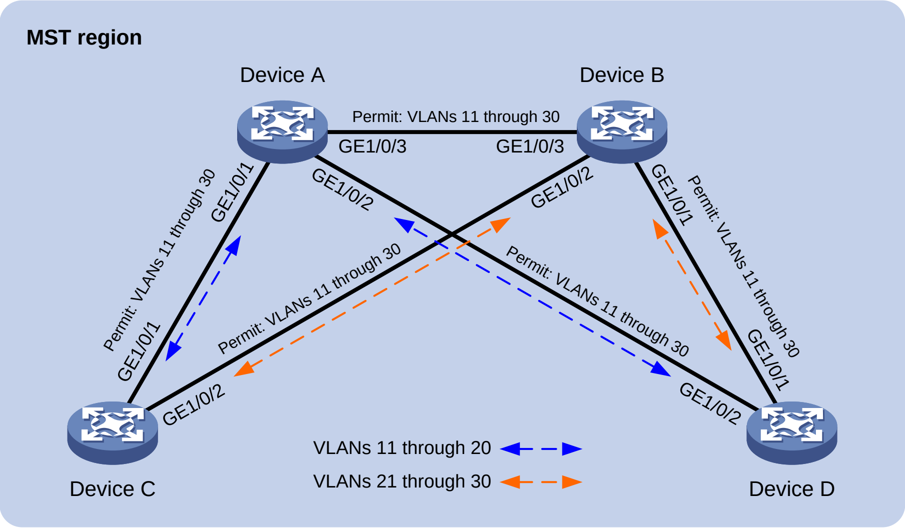
Network configuration

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:

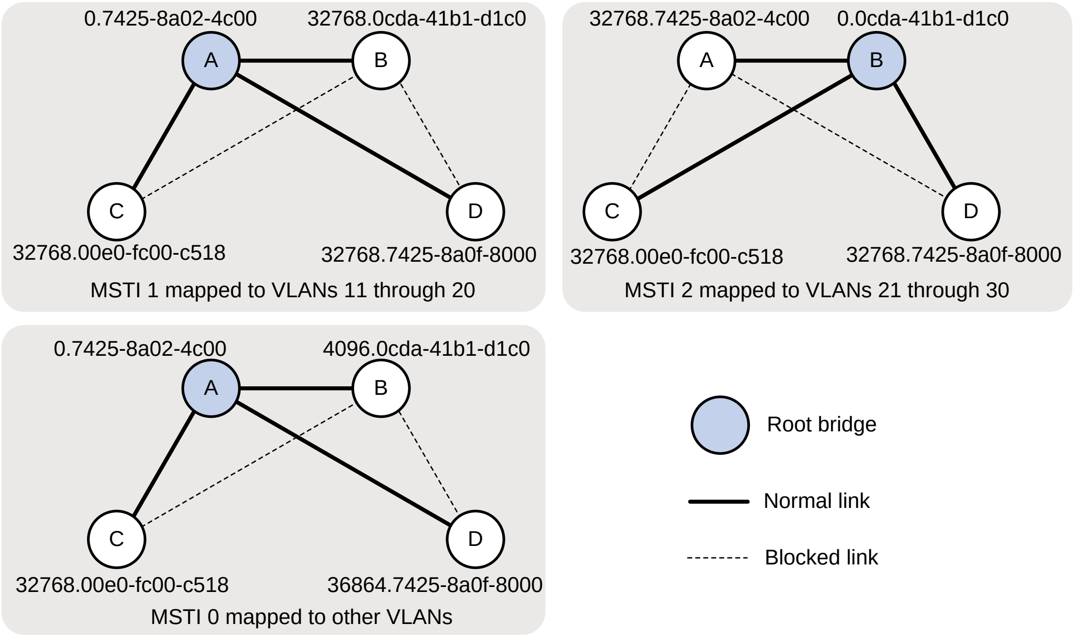
- Spanning tree mode (the default mode MSTP is used).
- Region name (**test** in this example).
- Revision level (the default value 0 is used).
- VLAN-to-instance mappings (VLANs 11 through 20 to MSTI 1, and VLANs 21 through 30 to MSTI 2).

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



Procedure

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
```

# Save the configuration.

```
[DeviceA] save force
```

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
```

# Save the configuration.

```
[DeviceB] save force
```

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
```

# Save the configuration.

```
[DeviceC] save force
```

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
```

# Save the configuration.

```
[DeviceD] save force
```

Verifying the configuration

1. Verify that Layer 2 loops have been eliminated in each MSTI:

   # 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                ALTE  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                ALTE  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.

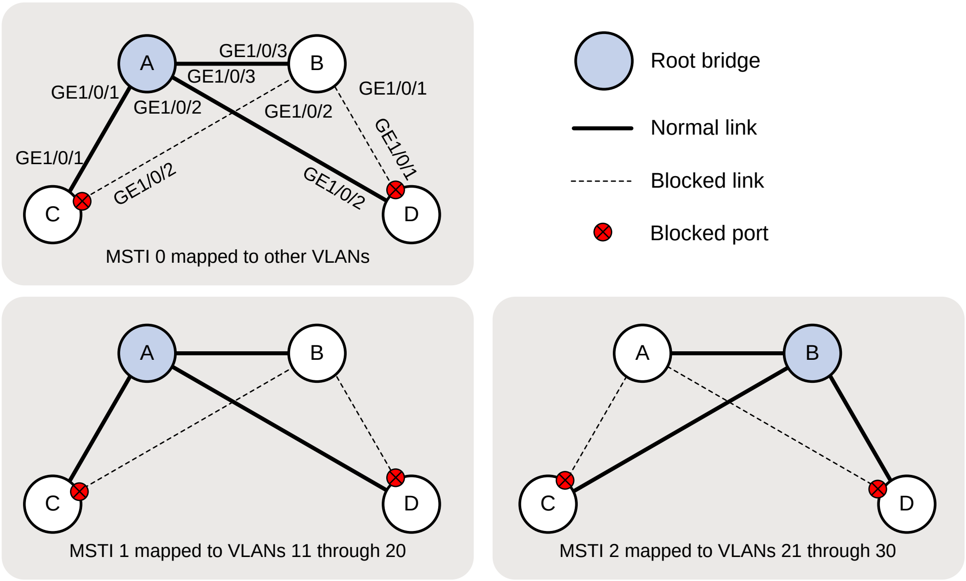
```
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  DISCARDING  NONE
 2        GigabitEthernet1/0/1                DESI  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



MSTI 0 mapped to other VLANs

MSTI 1 mapped to VLANs 11 through 20

MSTI 2 mapped to VLANs 21 through 30

2. Verify that the network can accommodate topology changes:

# Shut down GigabitEthernet 1/0/1 on Device C.

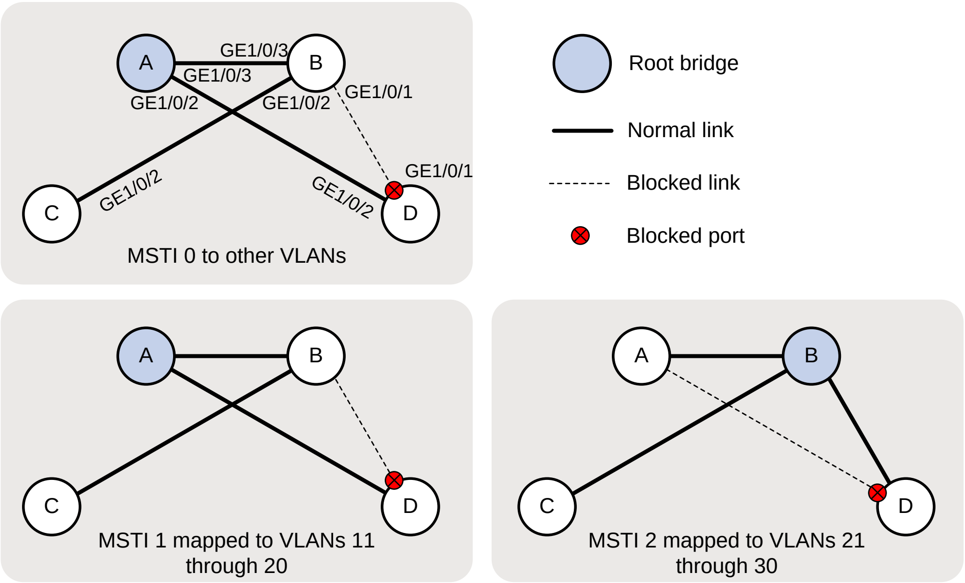
```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

# 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

- 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
```

Related documentation

- Spanning tree configuration in the Layer 2—LAN switching configuration guide for the device.
- Spanning tree commands in the Layer 2—LAN switching command reference for the device.

DHCP Quick Start Configuration Guide

Contents

Configuring dynamic IPv4 address assignment ··· 1

Introduction ······· 1
Network configuration ······· 1
Procedure······· 1
Verifying the configuration······· 3
Configuration files ······· 3
Related documentation ······· 4

Configuring DHCP relay agent······· 5

Introduction ······· 5
Network configuration ······· 5
Procedure······· 5
Verifying the configuration······· 7
Configuration files ······· 7
Related documentation ······· 8

Configuring DHCP snooping······· 9

Introduction ······· 9
Network configuration ······· 9
Procedure······· 9
Verifying the configuration······· 10
Configuration files ······· 10
Related documentation ······· 10

Configuring dynamic IPv6 address assignment ······· 11

Introduction ······· 11
Network configuration ······· 11
Procedure······· 11
Verifying the configuration······· 13
Configuration files ······· 14
Related documentation ······· 15

Configuring dynamic IPv4 address assignment

Introduction

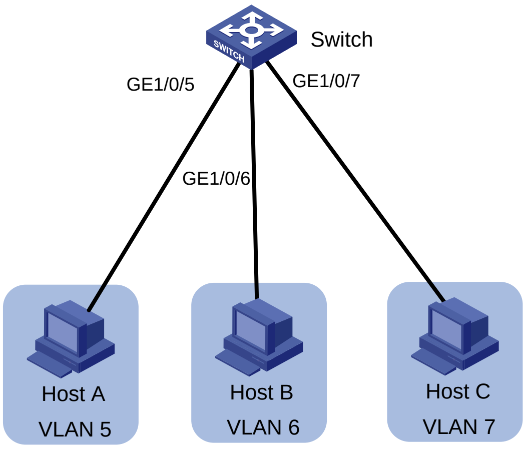
The following example describes the basic procedure to configure an interface as a DHCP server for dynamic IPv4 address assignment.

Network configuration

As shown in Figure 1, the core switch has three VLANs. Host A, Host B, and Host C are in VLAN 5, VLAN 6, and VLAN 7, respectively. Configure the core switch as a DHCP server to meet the following requirements:

- The clients on subnets 192.168.5.0/24, 192.168.6.0/24, and 192.168.7.0/24 can obtain IP addresses through DHCP.
- The IP addresses of VLAN-interface 5, VLAN-interface 6, and VLAN-interface 7 on the switch are 192.168.5.254/24, 192.168.6.254/24, and 192.168.7.254/24, respectively.
- For the hosts in subnet 192.168.5.0/24, the DNS server IP address is 192.168.5.100 and the gateway IP address is 192.168.5.254/24.
- For the hosts in subnet 192.168.6.0/24, the DNS server IP address is 192.168.6.100 and the gateway IP address is 192.168.6.254/24.
- For the hosts in subnet 192.168.7.0/24, the DNS server IP address is 192.168.7.100 and the gateway IP address is 192.168.7.254/24.

Figure 1 Network diagram



Procedure

# Enable DHCP on the switch.

```
<Switch> system-view
[Switch] dhcp enable
```

# Assign GigabitEthernet 1/0/5, GigabitEthernet 1/0/6, GigabitEthernet 1/0/7 to VLAN 5, VLAN 6, and VLAN 7, respectively.

```
[Switch] vlan 5
[Switch-vlan5] port gigabitEthernet 1/0/5
[Switch-vlan5] quit
[Switch]vlan 6
[Switch-vlan6] port gigabitEthernet 1/0/6
[Switch-vlan6] quit
[Switch]vlan 7
[Switch-vlan7] port gigabitEthernet 1/0/7
[Switch-vlan7] quit
```

# Assign IP addresses to VLAN-interface 5, VLAN-interface 6, and VLAN-interface 7. Each VLAN interface acts as the gateway in the VLAN to which the interface belongs.

```
[Switch] interface vlan-interface 5
[Switch-Vlan-interface5] ip address 192.168.5.254 255.255.255.0
[Switch-Vlan-interface5] quit
[Switch]interface vlan-interface 6
[Switch-Vlan-interface6] ip address 192.168.6.254 255.255.255.0
[Switch-Vlan-interface6] quit
[Switch]interface vlan-interface 7
[Switch-Vlan-interface7] ip address 192.168.7.254 255.255.255.0
[Switch-Vlan-interface7] quit
```

# (Optional.) Exclude specific IP addresses (such as DNS server IP addresses) from dynamic IP address assignment.

```
[Switch] dhcp server forbidden-ip 192.168.5.100
[Switch] dhcp server forbidden-ip 192.168.6.100
[Switch] dhcp server forbidden-ip 192.168.7.100
```

# Create IP address pool 5 to assign IP addresses to the clients on subnet 192.168.5.0/24.

```
[Switch] dhcp server ip-pool 5
[Switch-dhcp-pool-5] network 192.168.5.0 mask 255.255.255.0
[Switch-dhcp-pool-5] dns-list 192.168.5.100
[Switch-dhcp-pool-5] gateway-list 192.168.5.254
[Switch-dhcp-pool-5] quit
```

# Create IP address pool 6 to assign IP addresses to the clients on subnet 192.168.6.0/24.

```
[Switch] dhcp server ip-pool 6
[Switch-dhcp-pool-6] network 192.168.6.0 mask 255.255.255.0
[Switch-dhcp-pool-6] dns-list 192.168.6.100
[Switch-dhcp-pool-6] gateway-list 192.168.6.254
[Switch-dhcp-pool-6] quit
```

# Create IP address pool 7 to assign IP addresses to the clients on subnet 192.168.7.0/24.

```
[Switch] dhcp server ip-pool 7
[Switch-dhcp-pool-7] network 192.168.7.0 mask 255.255.255.0
[Switch-dhcp-pool-7] dns-list 192.168.7.100
[Switch-dhcp-pool-7] gateway-list 192.168.7.254
[Switch-dhcp-pool-7] quit
```

Verifying the configuration

# Check the IP addresses and other network settings of Host A, Host B, and Host C. Use the **display dhcp server ip-in-use** command to view the IP addresses assigned by the DHCP server.

```
[Switch] display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
192.168.5.1      0031-3865-392e-6262-  Jan 14 22:25:03 2021  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
192.168.6.2         0031-fe65-4203-7e02-  Jan 14 22:25:03 2021  Auto(C)
                 3063-5b30-3230-4702-
                 620e-712f-5e
192.168.7.3      3030-3030-2e30-3030-  Jan 9 10:45:11 2021   Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
```

The output shows that the DHCP server can assign IP addresses and other network settings to the clients on subnets 192.168.5.0/24, 192.168.6.0/24, and 192.168.7.0/24 correctly.

Configuration files

- Switch:

```
#
 dhcp enable
 dhcp server forbidden-ip 192.168.5.100
 dhcp server forbidden-ip 192.168.6.100
 dhcp server forbidden-ip 192.168.7.100
#
vlan 5 to 7
#
dhcp server ip-pool 5
 gateway-list 192.168.5.254
 network 192.168.5.0 mask 255.255.255.0
 dns-list 192.168.5.100
#
dhcp server ip-pool 6
 gateway-list 192.168.6.254
 network 192.168.6.0 mask 255.255.255.0
 dns-list 192.168.6.100
#
dhcp server ip-pool 7
 gateway-list 192.168.7.254
 network 192.168.7.0 mask 255.255.255.0
 dns-list 192.168.7.100
#
interface Vlan-interface5
```

```
 ip address 192.168.5.254 255.255.255.0
#
interface Vlan-interface6
 ip address 192.168.6.254 255.255.255.0
#
interface Vlan-interface7
 ip address 192.168.7.254 255.255.255.0
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 6
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port access vlan 7
#
```

Related documentation

- DHCP configuration in the Layer 3 IP services configuration guide for the device.
- DHCP commands in the Layer 3 IP services command reference for the device.

Configuring DHCP relay agent

Introduction

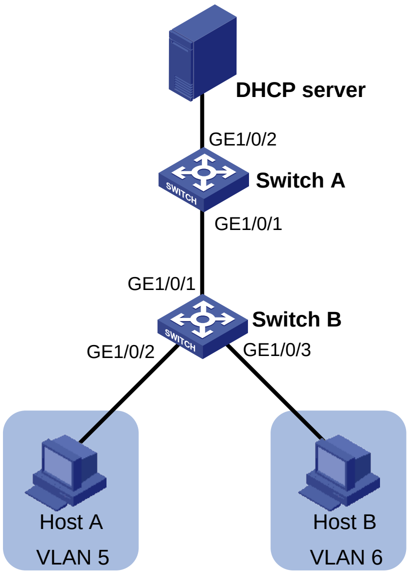
The following example describes the basic procedure to configure an interface as a DHCP relay agent. The DHCP relay agent enables clients to obtain IP addresses and configuration parameters from a DHCP server on another subnet.

Network configuration

As shown in Figure 2, Switch A acts as the core switch and has two VLANs. Host A and Host B are in VLAN 5 and VLAN 6, respectively. The DHCP server and the hosts run on different subnets and Switch A is the gateway for these hosts. Configure the network to meet the following requirements:

- The DHCP clients run on subnets 192.168.5.0/24 and 192.168.6.0/24, and the DHCP server IP address is 192.168.7.100/24.
- Switch A acts as the DHCP relay agent for clients, so these clients can obtain IP addresses in subnets 192.168.5.0/24 and 192.168.6.0/24, and other network settings from the DHCP server.

Figure 2 Network diagram



Procedure

1. Configure Switch B.

   # Create VLAN 5 and VLAN 6, and then assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 5 and VLAN 6, respectively.

```
<SwitchB> system-view
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitEthernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] vlan 6
```

```
[SwitchB-vlan6] port gigabitEthernet 1/0/3
[SwitchB-vlan6] quit
```

# Configure GigabitEthernet 1/0/1 as a trunk port, and allow packets from all VLANs to pass through the trunk port.

```
[SwitchB] interface gigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchB-GigabitEthernet1/0/1] quit
```

2. Configure Switch A.

# Enable DHCP.

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

# Create VLAN 5, VLAN 6, and VLAN 7, and then assign GigabitEthernet 1/0/2 to VLAN 7.

```
[SwitchA] vlan 5 to 7
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port access vlan 7
[SwitchA-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/1 as a trunk port, and allow packets from all VLANs to pass through the trunk port.

```
[SwitchA] interface gigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all
[SwitchA-GigabitEthernet1/0/1] quit
```

# Assign an IP address to VLAN 5, VLAN 6, and VLAN 7, respectively.

```
[SwitchA] interface vlan-interface 5
[SwitchA-Vlan-interface5] ip address 192.168.5.1 255.255.255.0
[SwitchA-Vlan-interface5] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 192.168.6.1 255.255.255.0
[SwitchA-Vlan-interface6] quit
[SwitchA]interface vlan-interface 7
[SwitchA-Vlan-interface7] ip address 192.168.7.1 255.255.255.0
[SwitchA-Vlan-interface7] quit
```

# Enable the DHCP relay agent mode on VLAN-interface 5.

```
[SwitchA] interface vlan-interface 5
[SwitchA-Vlan-interface5] dhcp select relay
```

# Assign IP address 192.168.7.100 to the DHCP server.

```
[SwitchA-Vlan-interface5] dhcp relay server-address 192.168.7.100
```

# Enable the DHCP relay agent mode on VLAN-interface 6.

```
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] dhcp select relay
```

# Assign IP address 192.168.7.100 to the DHCP server.

```
[SwitchA-Vlan-interface6] dhcp relay server-address 192.168.7.100
```

3. Configure DHCP server. Details are not shown.

# Assign IP address 192.168.7.100/24 to the NIC of the DHCP server.

# Configure IP address 192.168.7.1 as the gateway for the DHCP server.

# Make sure the DHCP server can ping 192.168.5.1 and 192.168.6.1.

Verifying the configuration

Check whether Host A and Host B can obtain IP addresses and other network settings from the DHCP server.

Configuration files

- Switch B:

```
#
vlan 5 to 6
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 6
```

- Switch A:

```
#
 dhcp enable
#
vlan 5 to 7
#
interface Vlan-interface5
 ip address 192.168.5.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 192.168.7.100
#
interface Vlan-interface6
 ip address 192.168.6.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 192.168.7.100
#
interface Vlan-interface7
 ip address 192.168.7.1 255.255.255.0
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
#
```

```
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 7
#
```

Related documentation

- DHCP configuration in the Layer 3 IP services configuration guide for the device.
- DHCP commands in the Layer 3 IP services command reference for the device.

Configuring DHCP snooping

Introduction

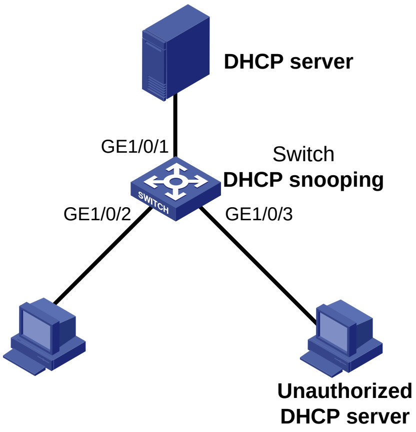
The following example describes the basic procedure to configure DHCP snooping.

Network configuration

As shown in Figure 3, the switch is connected to the authorized DHCP server through GigabitEthernet 1/0/1, to the unauthorized DHCP server through GigabitEthernet 1/0/3, and to the DHCP client through GigabitEthernet 1/0/2. Configure the network to meet the following requirements:

- Only the port connected to the authorized DHCP server can forward the responses from the DHCP server.
- The DHCP snooping device records clients' IP-to-MAC bindings by reading DHCP-ACK messages received from the trusted port and the DHCPREQUEST messages.

Figure 3 Network diagram



Procedure

# Enable global DHCP snooping.

```
<Switch> system-view
[Switch] dhcp snooping enable
```

# Configure GigabitEthernet 1/0/1 as a trusted port.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping trust
[Switch-GigabitEthernet1/0/1] quit
```

# Enable recording clients' IP-to-MAC bindings on GigabitEthernet 1/0/2.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] dhcp snooping binding record
[Switch-GigabitEthernet1/0/2] quit
```

Verifying the configuration

# Verify that the DHCP client can obtain an IP address and other configuration parameters only from the authorized DHCP server. (Details not shown.)

# Use the **display dhcp snooping binding** command to check the DHCP snooping entry recorded for the client.

Configuration files

```
#
 dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dhcp snooping trust
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 dhcp snooping binding record
#
```

Related documentation

- DHCP configuration in the Layer 3 IP services configuration guide for the device.
- DHCP commands in the Layer 3 IP services command reference for the device.

Configuring dynamic IPv6 address assignment

Introduction

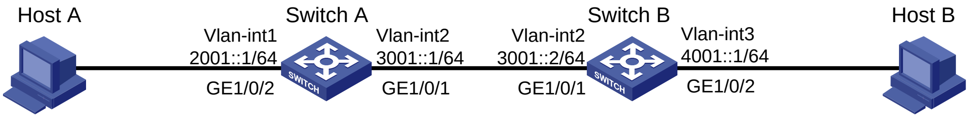
The following example describes the basic procedure to configure an interface as a DHCPv6 server for dynamic IPv6 address assignment.

Network configuration

As shown in Figure 4, Switch A and Switch B are gateway devices for internal hosts. Configure the network to meet the following requirements:

- Switch A and Switch B are connected through Ethernet interfaces. The interfaces of each switch operate in different VLAN and have IPv6 addresses.
- VLAN-interface 1 and VLAN-interface 3 operate in DHCPv6 server mode to assign IPv6 addresses to hosts.
- Switch A and Switch B have IPv6 static routes to ensure network connectivity.

Figure 4 Network diagram



Procedure

1. Configure Switch A.

   # Create VLAN 1 and assign GigabitEthernet 1/0/2 to VLAN 1.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 1
   [SwitchA-vlan1] port gigabitethernet 1/0/2
   [SwitchA-vlan1] quit
   ```

   # Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

   ```
   [SwitchA] vlan 2
   [SwitchA-vlan2] port gigabitethernet 1/0/1
   [SwitchA-vlan2] quit
   ```

   # Specify an IPv6 global unicast address for VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ipv6 address 3001::1/64
   [SwitchA-Vlan-interface2] quit
   ```

   # Specify an IPv6 global unicast address for VLAN-interface 1 and disable RA message suppression on VLAN-interface 1.

   ```
   [SwitchA] interface vlan-interface 1
   [SwitchA-Vlan-interface1] ipv6 address 2001::1/64
   ```

```
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
```

# Apply an IPv6 address pool to VLAN-interface 1.

```
[SwitchA-Vlan-interface1] ipv6 dhcp server apply pool 1 allow-hint rapid-commit
```

# Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 1. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.

```
[SwitchA-Vlan-interface1] ipv6 nd autoconfig managed-address-flag
```

# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 1. Hosts that receive the RA advertisements will obtain configuration information other than IPv6 address through DHCPv6.

```
[SwitchA-Vlan-interface1] ipv6 nd autoconfig other-flag
```

# Configure VLAN-interface 1 to operate in DHCPv6 server mode.

```
[SwitchA-Vlan-interface1] ipv6 dhcp select server
[SwitchA-Vlan-interface1] quit
```

# Create IPv6 address pool 1.

```
[SwitchA] ipv6 dhcp pool 1
[SwitchA-dhcp6-pool-1] network 2001::/64
[SwitchA-dhcp6-pool-1] dns-server 1::1
[SwitchA-dhcp6-pool-1] quit
```

# Configure an IPv6 static route destined for 4001::/64 and the next hop of the route is 3001::2.

```
[SwitchA] ipv6 route-static 4001:: 64 3001::2
```

# Save the configuration.

```
[SwitchA] save force
```

2. Configure Switch B.

# Create VLAN 2 and assign GigabitEthernet 1/0/1 to VLAN 2.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
```

# Create VLAN 3 and assign GigabitEthernet 1/0/2 to VLAN 3.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
```

# Specify an IPv6 global unicast address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

# Specify an IPv6 global unicast address for VLAN-interface 3 and disable RA message suppression on VLAN-interface 3.

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 4001::1/64
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

# Apply an IPv6 address pool to VLAN-interface 3.

```
[SwitchB-Vlan-interface3] ipv6 dhcp server apply pool 1 allow-hint rapid-commit
```

# Set the M flag to 1 in RA advertisements to be sent on VLAN-interface 3. Hosts that receive the RA advertisements will obtain IPv6 addresses through DHCPv6.

```
[SwitchB-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
```

# Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 3. Hosts that receive the RA advertisements will obtain configuration information other than IPv6 address through DHCPv6.

```
[SwitchB-Vlan-interface3] ipv6 nd autoconfig other-flag
```

# Configure VLAN-interface 3 to operate in DHCPv6 server mode.

```
[SwitchB-Vlan-interface3] ipv6 dhcp select server
[SwitchB-Vlan-interface3] quit
```

# Create IPv6 address pool 1.

```
[SwitchB] ipv6 dhcp pool 1
[SwitchB-dhcp6-pool-1] network 4001::/64
[SwitchB-dhcp6-pool-1] dns-server 1::1
[SwitchB-dhcp6-pool-1] quit
```

# Configure an IPv6 static route destined for 2001::/64 and the next hop of the route is 3001::1.

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

# Save the configuration.

```
[SwitchB] save force
```

3. Configure Host A.

   Configure IPv6 on Host A, and then enable Host A to use DHCPv6 for IPv6 address acquisition.

4. Configure Host B.

   Configure IPv6 on Host B, and then enable Host B to use DHCPv6 for IPv6 address acquisition.

Verifying the configuration

# View the IPv6 addresses assigned by the DHCPv6 server on Switch A.

```
[SwitchA] display ipv6 dhcp server ip-in-use
Pool: 1
 IPv6 address                                 Type      Lease expiration
 2001::2                                      Auto(C)   Sep 30 11:45:07 2021
```

# View information about the neighbors of GigabitEthernet 1/0/2 on Switch A.

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
2001::2                   b025-0b54-0106 --         GE1/0/2       REACH D  29
FE80::B225:BFF:FE54:106   b025-0b54-0106 --         GE1/0/2       REACH D  18
```

The output shows that Host A has obtained IPv6 global unicast address 2001::2.

# View the IPv6 addresses assigned by the DHCPv6 server on Switch B.

```
[SwitchB] display ipv6 dhcp server ip-in-use
Pool: 1
 IPv6 address                                 Type      Lease expiration
 4001::2                                      Auto(C)   Sep 30 14:05:49 2021
```

# View information about the neighbors of GigabitEthernet 1/0/2 on Switch B.

```
[SwitchB] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
4001::2                   b043-5415-0406 --         GE1/0/2       REACH D  3
FE80::B243:54FF:FE15:406  b043-5415-0406 --         GE1/0/2       REACH D  44
```

The output shows that Host B has obtained IPv6 global unicast address 4001::2.

# Check whether Host A and Host B can ping each other successfully.

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2
#
ipv6 dhcp pool 1
 network 2001::/64
 dns-server 1::1
#
interface Vlan-interface1
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1 allow-hint rapid-commit
 ipv6 address 2001::1/64
 ipv6 nd autoconfig managed-address-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface2
 ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
#
 ipv6 route-static 4001:: 64 3001::2
#
```

- Switch B:

```
#
vlan 2 to 3
#
ipv6 dhcp pool 1
 network 4001::/64
 dns-server 1::1
#
interface Vlan-interface2
 ipv6 address 3001::2/64
#
interface Vlan-interface3
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1 allow-hint rapid-commit
 ipv6 address 4001::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 ipv6 route-static 2001:: 64 3001::1
#
```

Related documentation

- DHCPv6 configuration in the Layer 3 IP services configuration guide for the device.
- DHCPv6 commands in the Layer 3 IP services command reference for the device.

OSPF Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring OSPF route redistribution ········· 1

Introduction ········· 1
Network configuration ········· 1
Data preparation ········· 1
Procedure········· 2
Verifying the configuration········· 6
Configuration files ········· 6
Related documentation ········· 9

Configuring basic OSPF in a single area ········· 10

Introduction ········· 10
Network configuration ········· 10
Procedure········· 10
Verifying the configuration········· 11
Configuration files ········· 13
Related documentation ········· 14

Configuring basic OSPF across multiple areas········· 15

Introduction ········· 15
Network configuration ········· 15
Data preparation ········· 15
Procedure········· 16
Verifying the configuration········· 19
Configuration files ········· 20
Related documentation ········· 22

Configuring OSPF route redistribution

Introduction

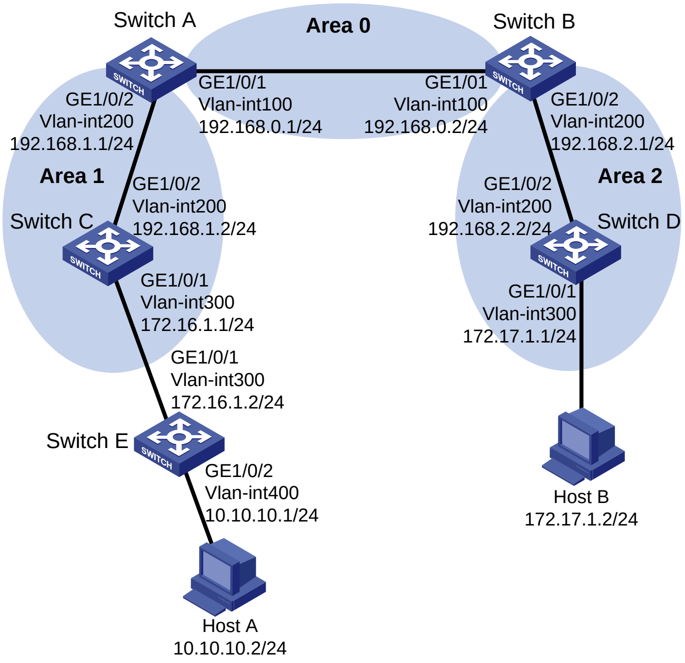
The following example describes the basic procedure to configure OSPF route redistribution.

Network configuration

As shown in Figure 1, Switch A, Switch B, Switch C, and Switch D run OSPF. Switch C and Switch E are configured with static routes. The AS is split into three areas. Configure the network to meet the following requirements:

- Switch A and Switch B act as ABRs.
- Switch C acts as an ASBR to redistribute external routes (static routes) and correctly advertise routes within the AS.

Figure 1 Network diagram



Data preparation

Device	Router ID	Interface and IP address	Subnet and OSPF area
Switch A	1.1.1.1	Physical interface: GE1/0/1 VLAN: 100 IP address: 192.168.0.1/24	Subnet: 192.168.0.0/24 OSPF area: area 0
		Physical interface: GE1/0/2 VLAN: 200	Subnet: 192.168.1.0/24 OSPF area: area 1

		IP address: 192.168.1.1/24	
Switch B	2.2.2.2	Physical interface: GE1/0/1 VLAN: 100 IP address: 192.168.0.2/24	Subnet: 192.168.0.0/24 OSPF area: area 0
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.2.1/24	Subnet: 192.168.2.0/24 OSPF area: area 2
Switch C	3.3.3.3	Physical interface: GE1/0/1 VLAN: 300 IP address: 172.16.1.1/24	Subnet: 172.16.1.0/24 OSPF area: area 1
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.1.2/24	Subnet: 192.168.1.0/24 OSPF area: area 1
Switch D	4.4.4.4	Physical interface: GE1/0/1 VLAN: 300 IP address: 172.17.1.1/24	Subnet: 172.17.1.0/24 OSPF area: area 2
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.2.2/24	Subnet: 192.168.2.0/24 OSPF area: area 2
Switch E	N/A	Physical interface: GE1/0/1 VLAN: 300 IP address: 172.16.1.2/24	Subnet: 172.16.1.0/24
		Physical interface: GE1/0/2 VLAN: 400 IP address: 10.10.10.1/24	Subnet: 10.10.10.0/24
Host A	N/A	IP address: 10.10.10.2/24	Subnet: 10.10.10.0/24
Host B	N/A	IP address: 172.17.1.2/24	Subnet: 172.17.1.0/24

Procedure

1. Configure Switch A.

   # Create VLAN 100 and assign GE1/0/1 to VLAN 100.

   ```
   <Switch A> system-view
   [Switch A] vlan 100
   [Switch A-vlan100] port gigabitethernet 1/0/1
   [Switch A-vlan100] quit
   ```

   # Create VLAN 200 and assign GE1/0/2 to VLAN 200.

   ```
   [Switch A] vlan 200
   ```

```
[Switch A-vlan200] port gigabitethernet 1/0/2
[Switch A-vlan200] quit
```

# Assign IP address 192.168.0.1/24 to VLAN-interface 100 and IP address 192.168.1.1/24 to VLAN-interface 200.

```
[Switch A] interface vlan 100
[Switch A-Vlan-interface100] ip address 192.168.0.1 255.255.255.0
[Switch A-Vlan-interface100] quit
[Switch A] interface vlan 200
[Switch A-Vlan-interface200] ip address 192.168.1.1 255.255.255.0
[Switch A-Vlan-interface200] quit
```

# Configure 1.1.1.1 as the global router ID for Switch A.

```
[Switch A] router id 1.1.1.1
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.0.0/24.

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
```

# Create area 1, and then advertise subnet 192.168.1.0/24.

```
[Switch A-ospf-1] area 1
[Switch A-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch A-ospf-1] quit
```

# Save the configuration.

```
[Switch A] save force
```

2. Configure Switch B.

# Create VLAN 100 and assign GE1/0/1 to VLAN 100.

```
<Switch B> system-view
[Switch B] vlan 100
[Switch B-vlan100] port gigabitethernet 1/0/1
[Switch B-vlan100] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch B] vlan 200
[Switch B-vlan200] port gigabitethernet 1/0/2
[Switch B-vlan200] quit
```

# Assign IP address 192.168.0.2/24 to VLAN-interface 100 and IP address 192.168.2.1/24 to VLAN-interface 200.

```
[Switch B] interface vlan 100
[Switch B-Vlan-interface100] ip address 192.168.0.2 255.255.255.0
[Switch B-Vlan-interface100] quit
[Switch B] interface vlan 200
[Switch B-Vlan-interface200] ip address 192.168.2.1 255.255.255.0
[Switch B-Vlan-interface200] quit
```

# Configure 2.2.2.2 as the global router ID for Switch B.

```
[Switch B] router id 2.2.2.2
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.0.0/24.

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
```

```
[Switch B-ospf-1-area-0.0.0.0] quit
```

# Create area 2, and then advertise subnet 192.168.2.0/24.

```
[Switch B-ospf-1] area 2
[Switch B-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.2] quit
[Switch B-ospf-1] quit
```

# Save the configuration.

```
[Switch B] save force
```

3. Configure Switch C.

# Create VLAN 300 and assign GE1/0/1 to VLAN 300.

```
<Switch C> system-view
[Switch C] vlan 300
[Switch C-vlan300] port gigabitethernet 1/0/1
[Switch C-vlan300] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch C] vlan 200
[Switch C-vlan200] port gigabitethernet 1/0/2
[Switch C-vlan200] quit
```

# Assign IP address 172.16.1.1/24 to VLAN-interface 300 and IP address 192.168.1.2/24 to VLAN-interface 200.

```
[Switch C] interface vlan 300
[Switch C-Vlan-interface300] ip address 172.16.1.1 255.255.255.0
[Switch C-Vlan-interface300] quit
[Switch C] interface vlan 200
[Switch C-Vlan-interface200] ip address 192.168.1.2 255.255.255.0
[Switch C-Vlan-interface200] quit
```

# Configure a static route destined for subnet 10.10.10.0/24 and the next hop of the route is 172.16.1.2.

```
[Switch C] ip route-static 10.10.10.0 24 172.16.1.2
```

# Configure 3.3.3.3 as the global router ID for Switch C.

```
[Switch C] router id 3.3.3.3
```

# Enable OSPF process 1, create area 1, and then advertise subnet 192.168.1.0/24 and subnet 172.16.1.0/24.

```
[Switch C] ospf 1
[Switch C-ospf-1] area 1
[Switch C-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] quit
```

# Enable OSPF to redistribute static routes.

```
[Switch C-ospf-1] import-route static
[Switch C-ospf-1] quit
```

# Save the configuration.

```
[Switch C] save force
```

4. Configure Switch D.

# Create VLAN 300 and assign GE1/0/1 to VLAN 300.

```
<Switch D> system-view
[Switch D] vlan 300
```

```
[Switch D-vlan300] port gigabitethernet 1/0/1
[Switch D-vlan300] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch D] vlan 200
[Switch D-vlan200] port gigabitethernet 1/0/2
[Switch D-vlan200] quit
```

# Assign IP address 172.17.1.1/24 to VLAN-interface 300 and IP address 192.168.2.2/24 to VLAN-interface 200.

```
[Switch D] interface vlan 300
[Switch D-Vlan-interface300] ip address 172.17.1.1 255.255.255.0
[Switch D-Vlan-interface300] quit
[Switch D] interface vlan 200
[Switch D-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch D-Vlan-interface200] quit
```

# Configure 4.4.4.4 as the global router ID for Switch D.

```
[Switch D] router id 4.4.4.4
```

# Enable OSPF process 1, create area 2, and then advertise subnet 192.168.2.0/24 and subnet 172.17.1.0/24.

```
[Switch D] ospf 1
[Switch D-ospf-1] area 2
[Switch D-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] quit
[Switch D-ospf-1] quit
```

# Save the configuration.

```
[Switch D] save force
```

5. Configure Switch E.

# Create VLAN 300 and assign GE1/0/1 to VLAN 300.

```
<Switch E> system-view
[Switch E] vlan 300
[Switch E-vlan300] port gigabitethernet 1/0/1
[Switch E-vlan300] quit
```

# Create VLAN 400 and assign GE1/0/2 to VLAN 400.

```
[Switch E] vlan 400
[Switch E-vlan400] port gigabitethernet 1/0/2
[Switch E-vlan400] quit
```

# Assign IP address 172.16.1.2/24 to VLAN-interface 300 and IP address 10.10.10.1/24 to VLAN-interface 400.

```
[Switch E] interface vlan 300
[Switch E-Vlan-interface300] ip address 172.16.1.2 255.255.255.0
[Switch E-Vlan-interface300] quit
[Switch E] interface vlan 400
[Switch E-Vlan-interface400] ip address 10.10.10.1 255.255.255.0
[Switch E-Vlan-interface400] quit
```

# Configure the default route and the next hop of the route is 172.16.1.1

```
[Switch E] ip route-static 0.0.0.0 0 172.16.1.1
```

# Save the configuration.

```
    [Switch E] save force
```

Verifying the configuration

# Use the **display ip routing-table** command to view the routing table of Switch A.

```
[Switch A] display ip routing-table
Destinations : 20       Routes : 20

Destination/Mask   Proto   Pre Cost        NextHop         Interface

0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.10.10.0/24      O_ASE2  150 1           192.168.1.2     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
172.16.1.0/24      O_INTRA 10  2           192.168.1.2     Vlan200
172.17.1.0/24      O_INTER 10  3           192.168.0.2     Vlan100
192.168.0.0/24     Direct  0   0           192.168.0.1     Vlan100
192.168.0.0/32     Direct  0   0           192.168.0.1     Vlan100
192.168.0.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.0.255/32   Direct  0   0           192.168.0.1     Vlan100
192.168.1.0/24     Direct  0   0           192.168.1.1     Vlan200
192.168.1.0/32     Direct  0   0           192.168.1.1     Vlan200
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     Vlan200
192.168.2.0/24     O_INTER 10  2           192.168.0.2     Vlan100
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 Switch A has routes to 172.16.1.0, 172.17.1.0, and 192.168.2.0 and has static routes that are redistributed from other routing protocols.

# Check whether Host A can ping Host B successfully.

```
C:\Users\HostA>ping 172.17.1.2
```

The output shows that Host A can ping Host B successfully.

Configuration files

- Switch A:

```
#
 router id 1.1.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
```

```
  network 192.168.1.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch B:

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch C:

```
#
 router id 3.3.3.3
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
```

```
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch D:

```
#
 router id 4.4.4.4
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch E:

```
#
interface Vlan-interface200
 ip address 10.10.10.1 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
 ip route-static 0.0.0.0 0 172.16.1.1
#
```

Related documentation

- OSPF configuration in the Layer 3—IP routing configuration guide for the device.
- OSPF commands in the Layer 3—IP routing command reference for the device.

Configuring basic OSPF in a single area

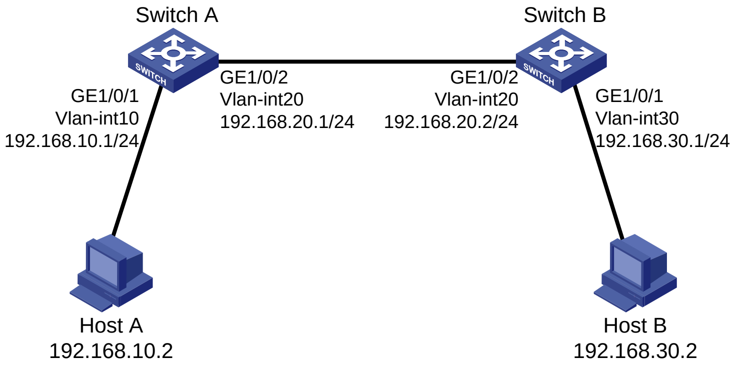
Introduction

The following example describes the procedure to configure basic OSPF in a single area.

Network configuration

As shown in Figure 2, Switch A and Switch B run OSPF. Configure the network to ensure that Host A and Host B can access each other through Switch A and Switch B.

Figure 2 Network diagram



Procedure

1. Configure Switch A.

   # Create VLAN 10 and assign GE1/0/1 to VLAN 10.

```
<Switch A> system-view
[Switch A] vlan 10
[Switch A-vlan10] port gigabitethernet 1/0/1
[Switch A-vlan10] quit
```

   # Create VLAN 20 and assign GE1/0/2 to VLAN 20.

```
[Switch A] vlan 20
[Switch A-vlan20] port gigabitethernet 1/0/2
[Switch A-vlan20] quit
```

   # Assign IP address 192.168.10.1/24 to VLAN-interface 10 and IP address 192.168.20.1/24 to VLAN-interface 20.

```
[Switch A] interface vlan 10
[Switch A-Vlan-interface10] ip address 192.168.10.1 255.255.255.0
[Switch A-Vlan-interface10] quit
[Switch A] interface vlan 20
[Switch A-Vlan-interface20] ip address 192.168.20.1 255.255.255.0
[Switch A-Vlan-interface20] quit
```

   # Configure 1.1.1.1 as the global router ID for Switch A.

```
[Switch A] router id 1.1.1.1
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.10.0/24 and subnet 192.168.20.0/24.

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
[Switch A-ospf-1] quit
```

# Save the configuration.

```
[Switch A] save force
```

2. Configure Switch B.

# Create VLAN 30 and assign GE1/0/1 to VLAN 30.

```
<Switch B> system-view
[Switch B] vlan 30
[Switch B-vlan30] port gigabitethernet 1/0/1
[Switch B-vlan30] quit
```

# Create VLAN 20 and assign GE1/0/2 to VLAN 20.

```
[Switch B] vlan 20
[Switch B-vlan20] port gigabitethernet 1/0/2
[Switch B-vlan20] quit
```

# Assign IP address 192.168.30.1/24 to VLAN-interface 30 and IP address 192.168.20.2/24 to VLAN-interface 20.

```
[Switch B] interface vlan 30
[Switch B-Vlan-interface30] ip address 192.168.30.1 255.255.255.0
[Switch B-Vlan-interface30] quit
[Switch B] interface vlan 20
[Switch B-Vlan-interface20] ip address 192.168.20.2 255.255.255.0
[Switch B-Vlan-interface20] quit
```

# Configure 2.2.2.2 as the global router ID for Switch B.

```
[Switch B] router id 2.2.2.2
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.20.0/24 and subnet 192.168.30.0/24.

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] network 192.168.30.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] quit
[Switch B-ospf-1] quit
```

# Save the configuration.

```
[Switch B] save force
```

Verifying the configuration

# Use the **display ospf peer** command to view the OSPF neighbors of Switch A.

```
[Switch A] display ospf peer
```

```
         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         192.168.20.2    1   30         Full/DR -         Vlan20
```

# Use the **`display ospf routing`** command to view the OSPF routes of Switch A.

```
[Switch A] 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
 192.168.10.0/24    1        Stub    0.0.0.0         192.168.20.1    0.0.0.0
 192.168.30.0/24    2        Stub    192.168.20.2    192.168.20.2    0.0.0.0
 192.168.20.0/24    1        Transit 0.0.0.0         192.168.20.1    0.0.0.0
```

# Use the **`display ip routing-table`** command to view the routing table of Switch A.

```
[Switch A] display ip routing-table

Destinations : 17       Routes : 17

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
127.0.0.0/32       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
192.168.10.0/24    Direct  0   0           192.168.10.1    Vlan10
192.168.10.0/32    Direct  0   0           192.168.10.1    Vlan10
192.168.10.1/32    Direct  0   0           127.0.0.1       InLoop0
192.168.10.255/32  Direct  0   0           192.168.10.1    Vlan10
192.168.20.0/24    Direct  0   0           192.168.20.1    Vlan20
192.168.20.0/32    Direct  0   0           192.168.20.1    Vlan20
192.168.20.1/32    Direct  0   0           127.0.0.1       InLoop0
192.168.20.255/32  Direct  0   0           192.168.20.1    Vlan20
192.168.30.0/24    O_INTRA 10  2           192.168.20.2    Vlan20
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 Switch A has a route to 192.168.30.0/24.

# Check whether Host A can ping Host B successfully.

```
C:\Users\HostA>ping 192.168.30.2
```

The output shows that Host A can ping Host B successfully.

Configuration files

- Switch A:

```
#
 router id 1.1.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
```

- Switch B:

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.20.0 0.0.0.255
  network 192.168.30.0 0.0.0.255
#
interface Vlan-interface20
 ip address 192.168.20.2 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.30.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 30
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
```

Related documentation

- OSPF configuration in the Layer 3—IP routing configuration guide for the device.
- OSPF commands in the Layer 3—IP routing command reference for the device.

Configuring basic OSPF across multiple areas

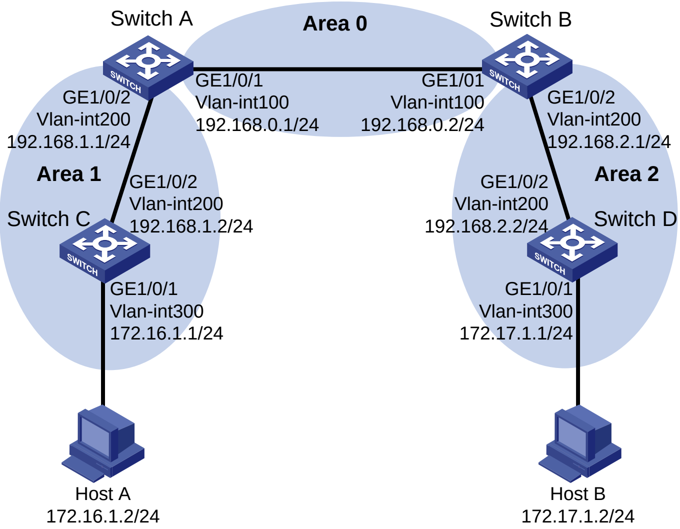
Introduction

The following example describes the procedure to configure basic OSPF across multiple areas.

Network configuration

As shown in Figure 3, Switch A, Switch B, Switch C, and Switch D run OSPF. The AS is split into three areas. Switch A and Switch B act as ABRs. Configure the network to ensure that each switch can learn all of the routes in the AS.

Figure 3 Network diagram



Data preparation

Device	Router ID	Interface and IP address	Subnet and OSPF area
Switch A	1.1.1.1	Physical interface: GE1/0/1 VLAN: 100 IP address: 192.168.0.1/24	Subnet: 192.168.0.0/24 OSPF area: area 0
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.1.1/24	Subnet: 192.168.1.0/24 OSPF area: area 1
Switch B	2.2.2.2	Physical interface: GE1/0/1 VLAN: 100	Subnet: 192.168.0.0/24 OSPF area: area 0

		IP address: 192.168.0.2/24	
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.2.1/24	Subnet: 192.168.2.0/24 OSPF area: area 2
Switch C	3.3.3.3	Physical interface: GE1/0/1 VLAN: 300 IP address: 172.16.1.1/24	Subnet: 172.16.1.0/24 OSPF area: area 1
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.1.2/24	Subnet: 192.168.1.0/24 OSPF area: area 1
Switch D	4.4.4.4	Physical interface: GE1/0/1 VLAN: 300 IP address: 172.17.1.1/24	Subnet: 172.17.1.0/24 OSPF area: area 2
		Physical interface: GE1/0/2 VLAN: 200 IP address: 192.168.2.2/24	Subnet: 192.168.2.0/24 OSPF area: area 2
Host A	N/A	IP address: 172.16.1.2/24	Subnet: 172.16.1.0/24
Host B	N/A	IP address: 172.17.1.2/24	Subnet: 172.17.1.0/24

Procedure

1. Configure Switch A.

   # Create VLAN 100 and assign GE1/0/1 to VLAN 100.

   ```
   <Switch A> system-view
   [Switch A] vlan 100
   [Switch A-vlan100] port gigabitethernet 1/0/1
   [Switch A-vlan100] quit
   ```

   # Create VLAN 200 and assign GE1/0/2 to VLAN 200.

   ```
   [Switch A] vlan 200
   [Switch A-vlan200] port gigabitethernet 1/0/2
   [Switch A-vlan200] quit
   ```

   # Assign IP address 192.168.0.1/24 to VLAN-interface 100 and IP address 192.168.1.1/24 to VLAN-interface 200.

   ```
   [Switch A] interface vlan 100
   [Switch A-Vlan-interface100] ip address 192.168.0.1 255.255.255.0
   [Switch A-Vlan-interface100] quit
   [Switch A] interface vlan 200
   [Switch A-Vlan-interface200] ip address 192.168.1.1 255.255.255.0
   [Switch A-Vlan-interface200] quit
   ```

   # Configure 1.1.1.1 as the global router ID for Switch A.

```
[Switch A] router id 1.1.1.1
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.0.0/24.

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
```

# Create area 1, and then advertise subnet 192.168.1.0/24.

```
[Switch A-ospf-1] area 1
[Switch A-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.1] quit
[Switch A-ospf-1] quit
```

# Save the configuration.

```
[Switch A] save force
```

2. Configure Switch B.

# Create VLAN 100 and assign GE1/0/1 to VLAN 100.

```
<Switch B> system-view
[Switch B] vlan 100
[Switch B-vlan100] port gigabitethernet 1/0/1
[Switch B-vlan100] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch B] vlan 200
[Switch B-vlan200] port gigabitethernet 1/0/2
[Switch B-vlan200] quit
```

# Assign IP address 192.168.0.2/24 to VLAN-interface 100 and IP address 192.168.2.1/24 to VLAN-interface 200.

```
[Switch B] interface vlan 100
[Switch B-Vlan-interface100] ip address 192.168.0.2 255.255.255.0
[Switch B-Vlan-interface100] quit
[Switch B] interface vlan 200
[Switch B-Vlan-interface200] ip address 192.168.2.1 255.255.255.0
[Switch B-Vlan-interface200] quit
```

# Configure 2.2.2.2 as the global router ID for Switch B.

```
[Switch B] router id 2.2.2.2
```

# Enable OSPF process 1, create area 0, and then advertise subnet 192.168.0.0/24.

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] quit
```

# Create area 2, and then advertise subnet 192.168.2.0/24.

```
[Switch B-ospf-1] area 2
[Switch B-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.2] quit
[Switch B-ospf-1] quit
```

# Save the configuration.

```
[Switch B] save force
```

3. Configure Switch C.

# Create VLAN 300 and assign GE1/0/1 to VLAN 300.

```
<Switch C> system-view
[Switch C] vlan 300
[Switch C-vlan300] port gigabitethernet 1/0/1
[Switch C-vlan300] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch C] vlan 200
[Switch C-vlan200] port gigabitethernet 1/0/2
[Switch C-vlan200] quit
```

# Assign IP address 172.16.1.1/24 to VLAN-interface 300 and IP address 192.168.1.2/24 to VLAN-interface 200.

```
[Switch C] interface vlan 300
[Switch C-Vlan-interface300] ip address 172.16.1.1 255.255.255.0
[Switch C-Vlan-interface300] quit
[Switch C] interface vlan 200
[Switch C-Vlan-interface200] ip address 192.168.1.2 255.255.255.0
[Switch C-Vlan-interface200] quit
```

# Configure 3.3.3.3 as the global router ID for Switch C.

```
[Switch C] router id 3.3.3.3
```

# Enable OSPF process 1, create area 1, and then advertise subnet 192.168.1.0/24 and subnet 172.16.1.0/24.

```
[Switch C] ospf 1
[Switch C-ospf-1] area 1
[Switch C-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] quit
[Switch C-ospf-1] quit
```

# Save the configuration.

```
[Switch C] save force
```

4. Configure Switch D.

# Create VLAN 300 and assign GE1/0/1 to VLAN 300.

```
<Switch D> system-view
[Switch D] vlan 300
[Switch D-vlan300] port gigabitethernet 1/0/1
[Switch D-vlan300] quit
```

# Create VLAN 200 and assign GE1/0/2 to VLAN 200.

```
[Switch D] vlan 200
[Switch D-vlan200] port gigabitethernet 1/0/2
[Switch D-vlan200] quit
```

# Assign IP address 172.17.1.1/24 to VLAN-interface 300 and IP address 192.168.2.2/24 to VLAN-interface 200.

```
[Switch D] interface vlan 300
[Switch D-Vlan-interface300] ip address 172.17.1.1 255.255.255.0
[Switch D-Vlan-interface300] quit
[Switch D] interface vlan 200
[Switch D-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch D-Vlan-interface200] quit
```

# Configure 4.4.4.4 as the global router ID for Switch D.

```
[Switch D] router id 4.4.4.4
```

# Enable OSPF process 1, create area 2, and then advertise subnet 192.168.2.0/24 and subnet 172.17.1.0/24.

```
[Switch D] ospf 1
[Switch D-ospf-1] area 2
[Switch D-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] quit
[Switch D-ospf-1] quit
```

# Save the configuration.

```
[Switch D] save force
```

Verifying the configuration

# Use the **display ospf peer** command to view the OSPF neighbors of Switch A.

```
[Switch A] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         192.168.0.2     1   33         Full/DR           Vlan100

 Area: 0.0.0.1
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         192.168.1.2     1   34         Full/DR           Vlan200
```

# Use the **display ip routing-table** command to view the routing table of Switch A.

```
[Switch A] 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
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
172.16.1.0/24      O_INTRA 10  2           192.168.1.2     Vlan200
172.17.1.0/24      O_INTER 10  3           192.168.0.2     Vlan100
192.168.0.0/24     Direct  0   0           192.168.0.1     Vlan100
192.168.0.0/32     Direct  0   0           192.168.0.1     Vlan100
192.168.0.1/32     Direct  0   0           127.0.0.1       InLoop0
192.168.0.255/32   Direct  0   0           192.168.0.1     Vlan100
192.168.1.0/24     Direct  0   0           192.168.1.1     Vlan200
192.168.1.0/32     Direct  0   0           192.168.1.1     Vlan200
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     Vlan200
192.168.2.0/24     O_INTER 10  2           192.168.0.2     Vlan100
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 Switch A has routes to 172.16.1.0, 172.17.1.0, and 192.168.2.0.

# Check whether Host A can ping Host B successfully.

```
C:\Users\HostA>ping 172.17.1.2
```

The output shows that Host A can ping Host B successfully.

Configuration files

- Switch A:

```
#
 router id 1.1.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch B:

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
```

```
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch C:

```
#
 router id 3.3.3.3
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch D:

```
#
 router id 4.4.4.4
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
```

```
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

Related documentation

- OSPF configuration in the Layer 3—IP routing configuration guide for the device.
- OSPF commands in the Layer 3—IP routing command reference for the device.

Static Routing Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring static routing-Track-NQA collaboration ······ 1

Introduction ······ 1
Network configuration ······ 1
Analysis ······ 2
Procedure ······ 2
Verifying the configuration ······ 6
Configuration files ······ 8
Related documentation ······ 11

Accessing the Web interface of a device in a different subnet ······ 12

Introduction ······ 12
Network configuration ······ 12
Procedure ······ 12
Verifying the configuration ······ 13
Configuration files ······ 14
Related documentation ······ 15

Configuring basic IPv6 static route settings ······ 16

Introduction ······ 16
Network configuration ······ 16
Procedure ······ 16
Verifying the configuration ······ 18
Configuration files ······ 19
Related documentation ······ 20

Configuring a default route ······ 21

Introduction ······ 21
Network configuration ······ 21
Procedure ······ 21
Verifying the configuration ······ 22
Configuration files ······ 22
Related documentation ······ 23

Configuring basic static route settings ······ 24

Introduction ······ 24
Network configuration ······ 24
Procedure ······ 24

Verifying the configuration 25
Configuration files 25
Related documentation 26

Configuring a floating static route 28

Introduction 28
Network configuration 28
Procedure 28
Verifying the configuration 31
Configuration files 32
Related documentation 35

Configuring static routing-Track-NQA collaboration

Introduction

The following information uses an example to describe the basic procedure for configuring static routing-Track-NQA collaboration.

Network configuration

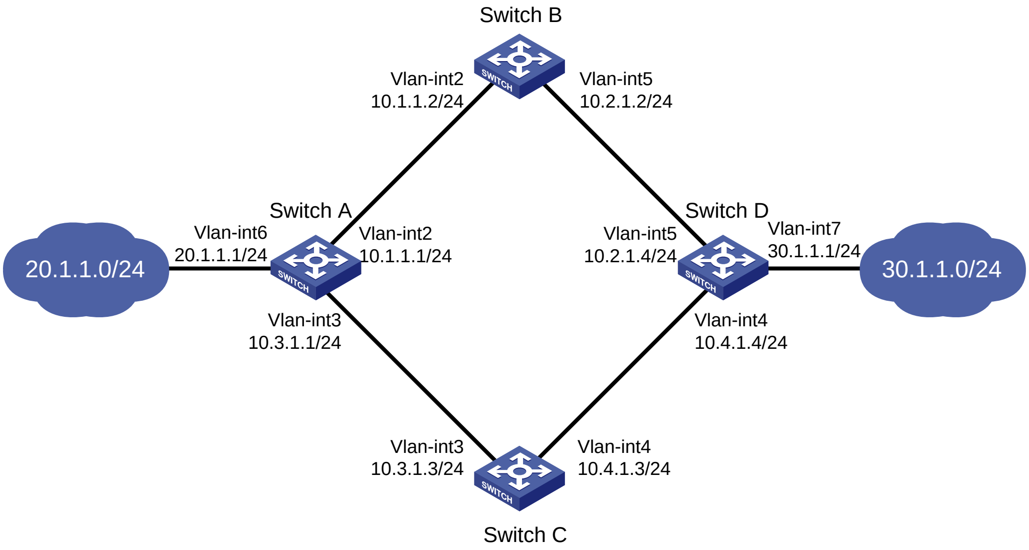
As shown in Figure 1:

- Switch A is the default gateway of the hosts in network 20.1.1.0/24.
- Switch D is the default gateway of the hosts in network 30.1.1.0/24.
- Hosts in the two networks communicate with each other through static routes.

To ensure network availability, configure route backup and static routing-Track-NQA collaboration on Switch A and Switch D as follows:

- On Switch A, assign a higher priority to the static route to 30.1.1.0/24 with next hop Switch B. This route is the master route. The static route to 30.1.1.0/24 with next hop Switch C acts as the backup route. When the master route is unavailable, the backup route takes effect. Switch A forwards packets to 30.1.1.0/24 through Switch C.
- On Switch D, assign a higher priority to the static route to 20.1.1.0/24 with next hop Switch B. This route is the master route. The static route to 20.1.1.0/24 with next hop Switch C acts as the backup route. When the master route is unavailable, the backup route takes effect. Switch D forwards packets to 20.1.1.0/24 through Switch C.

Figure 1 Network diagram



Analysis

1. Assign IP address to the devices.
2. Configure static routes:

   Assign a higher priority to the static route with Switch B as the next hop (master route) than the static route with Switch C as the next hop (backup route).
3. Configure NQA operations:

   Configure NQA operations on Switch A and Switch D to test the connectivity of the path Switch A-Switch B-Switch D. Associate Track with the NQA operations to implement collaboration between static routing, Track, and NQA.

Procedure

Configuring Switch A

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 6
[SwitchA-vlan6] port gigabitethernet 1/0/3
```

```
[SwitchA-vlan6] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.3.1.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 20.1.1.1 24
[SwitchA-Vlan-interface6] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.1.1.2 and the default priority (60). Associate this static route with track entry 1.

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

# Configure a static route to 30.1.1.0/24 with next hop 10.3.1.3 and priority 80.

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

# Configure a static route to 10.2.1.4 with next hop 10.1.1.2.

```
[SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
```

# Create an NQA operation with administrator name **admin** and operation tag **test**.

```
[SwitchA] nqa entry admin test
```

# Specify the ICMP echo operation type.

```
[SwitchA-nqa-admin-test] type icmp-echo
```

# Specify 10.2.1.4 as the destination address of the operation and specify 10.1.1.2 as the next hop of the operation to detect connectivity of the path Switch A-Switch B-Switch D.

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
[SwitchA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```

# Configure the ICMP echo operation to repeat every 100 milliseconds.

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

# Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```

# Start the NQA operation.

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# Configure track entry 1, and associate it with reaction entry 1 of the NQA operation.

```
[SwitchA] track 1 nqa entry admin test reaction 1
[SwitchA-track-1] quit
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchB> system-view
```

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 24
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 10.2.1.2 24
[SwitchB-Vlan-interface5] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.2.1.4.

```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

# Configure a static route to 20.1.1.0/24 with next hop 10.1.1.1.

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring Switch C

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] quit
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/2
[SwitchC-vlan4] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 10.3.1.3 24
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 10.4.1.3 24
[SwitchC-Vlan-interface4] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.4.1.4.

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

# Configure a static route to 20.1.1.0/24 with next hop 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

# Save the configuration.

```
[SwitchC] save force
```

Configuring Switch D

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchD> system-view
[SwitchD] vlan 4
```

```
[SwitchD-vlan4] port gigabitethernet 1/0/1
[SwitchD-vlan4] quit
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/2
[SwitchD-vlan5] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface6] ip address 10.4.1.4 24
[SwitchD-Vlan-interface6] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 10.2.1.4 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 30.1.1.1 24
[SwitchD-Vlan-interface7] quit
```

# Configure a static route to 20.1.1.0/24 with next hop 10.2.1.2 and the default priority (60). Associate this static route with track entry 1.

```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

# Configure a static route to 20.1.1.0/24 with next hop 10.4.1.3 and priority 80.

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

# Configure a static route to 10.1.1.1 with next hop 10.2.1.2.

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

# Create an NQA operation with administrator name **admin** and operation tag **test**.

```
[SwitchD] nqa entry admin test
```

# Specify the ICMP echo operation type.

```
[SwitchD-nqa-admin-test] type icmp-echo
```

# Specify 10.1.1.1 as the destination address of the operation and specify 10.2.1.2 as the next hop of the operation to detect connectivity of the path Switch D-Switch B-Switch A.

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2
```

# Configure the ICMP echo operation to repeat every 100 milliseconds.

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

# Configure reaction entry 1, specifying that five consecutive probe failures trigger the Track module.

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
```

# Start the NQA operation.

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

# Configure track entry 1, and associate it with reaction entry 1 of the NQA operation.

```
[SwitchD] track 1 nqa entry admin test reaction 1
[SwitchD-track-1] quit
```

# Save the configuration.

```
[SwitchD] save force
```

Verifying the configuration

# Display track entry information on Switch A.

```
[SwitchA] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: NQA
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL: 10.2.1.4
    Local IP: --
    Interface: --
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
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
```

The output shows that the status of the track entry is Positive, indicating that the NQA operation has succeeded and the master route is available. Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] undo ip address
```

# Display track entry information on Switch A.

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: NQA
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL: 10.2.1.4
    Local IP: --
    Interface: --
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
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
```

The output shows that the status of the track entry is Negative, indicating that the NQA operation has failed and the master route is unavailable. Switch A forwards packets to 30.1.1.0/24 through Switch C. The backup static route has taken effect.

# Verify that hosts in 20.1.1.0/24 can communicate with the hosts in 30.1.1.0/24 when the master route fails.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

# Verify associated information on Switch D (similar to that on Switch A). Verify that hosts in 30.1.1.0/24 can communicate with the hosts in 20.1.1.0/24 when the master route fails.

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Configuration files

- Switch A:

```
#
vlan 2
#
vlan 3
#
vlan 6
#
nqa entry admin test
 type icmp-echo
  destination ip 10.2.1.4
  frequency 100
  next-hop ip 10.1.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 nqa schedule admin test start-time now lifetime forever
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface6
 ip address 20.1.1.1 255.255.255.0
#
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 access vlan 6
#
 ip route-static 10.2.1.0 24 10.1.1.2
 ip route-static 30.1.1.0 24 10.1.1.2 track 1
 ip route-static 30.1.1.0 24 10.3.1.3 preference 80
#
 track 1 nqa entry admin test reaction 1
#
```

- Switch B:

```
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 20.1.1.0 24 10.1.1.1
 ip route-static 30.1.1.0 24 10.2.1.4
#
```

- Switch C:

```
#
vlan 3
#
vlan 4
#
interface Vlan-interface3
 ip address 10.3.1.3 255.255.255.0
#
interface Vlan-interface4
 ip address 10.4.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 4
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.4
#
```

- Switch D:

```
#
vlan 4
#
vlan 5
#
vlan 7
#
nqa entry admin test
 type icmp-echo
  destination ip 10.1.1.1
  frequency 100
  next-hop ip 10.2.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 nqa schedule admin test start-time now lifetime forever
#
interface Vlan-interface4
 ip address 10.4.1.4 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.4 255.255.255.0
#
interface Vlan-interface7
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
#
 ip route-static 10.1.1.0 24 10.2.1.2
 ip route-static 20.1.1.0 24 10.2.1.2 track 1
 ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

```
#
 track 1 nqa entry admin test reaction 1
#
```

Related documentation

- Static routing configuration in the Layer 3—IP routing configuration guide for the device.
- Static routing commands in the Layer 3—IP routing command reference for the device.
- Track configuration in the high availability configuration guide for the device.
- Track commands in the high availability command reference for the device.

Accessing the Web interface of a device in a different subnet

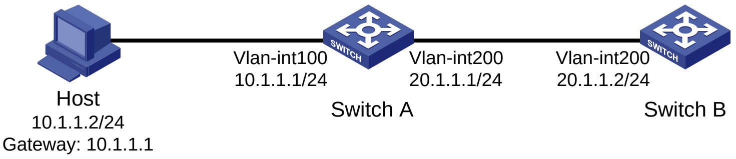
Introduction

The following information uses an example to describe the basic procedure for accessing the Web interface of a device in a different subnet.

Network configuration

As shown in Figure 2, the host is connected to the switches in an IP network and has a route to reach the switches. Enable the host to access the Web interface of Switch B through HTTP in a different subnet.

Figure 2 Network diagram



Procedure

Configuring Switch A

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] port gigabitethernet 1/0/2
[SwitchA-vlan200] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 20.1.1.1 24
[SwitchA-Vlan-interface200] quit
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create a VLAN and assign a port to it. Configure the IP address of the VLAN interface.

```
<SwitchB> system-view
[SwitchB] vlan 200
[SwitchB-vlan200] port gigabitethernet 1/0/1
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ip address 20.1.1.2 24
[SwitchB-Vlan-interface200] quit
```

# Configure username **admin**, authentication password **hello12345**, service type **http**, and user role **network-admin**.

```
[SwitchB] local-user admin
[SwitchB-luser-manage-admin] service-type http
[SwitchB-luser-manage-admin] authorization-attribute user-role network-admin
[SwitchB-luser-manage-admin] password simple hello12345
[SwitchB-luser-manage-admin] quit
```

# Enable the HTTP service.

```
[SwitchB] ip http enable
```

# Configure a static route.

```
[SwitchB] ip route-static 10.1.1.0 24 20.1.1.1
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring the host

# Configure IP address 10.1.1.2, subnet mask 255.255.255.0, and gateway address 10.1.1.1 for the host. (Details not shown.)

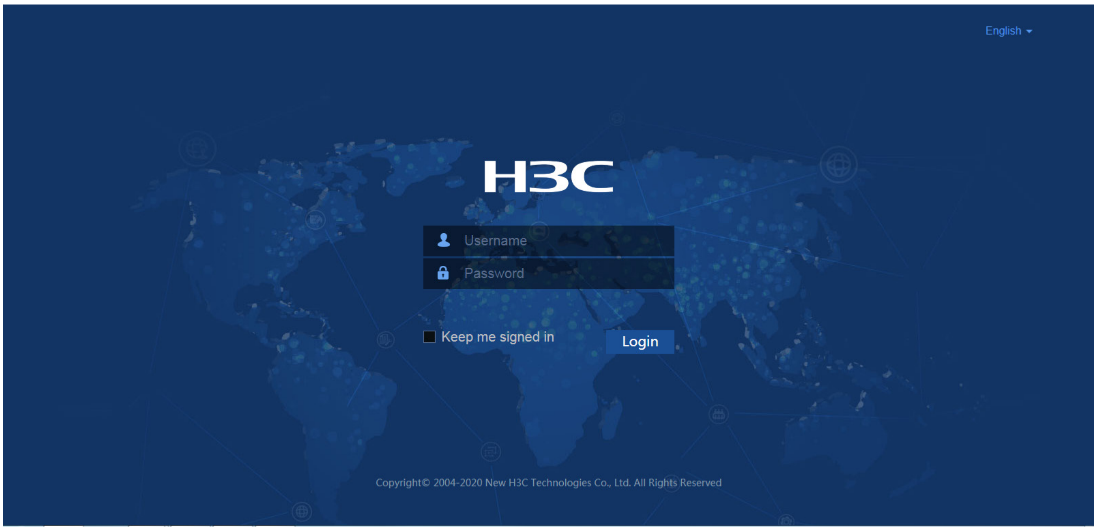
Verifying the configuration

# Ping Switch B on the host to verify that host can communicate with Switch B (assuming Windows XP is installed on the host).

```
C:\Documents and Settings\Administrator>ping 20.1.1.2

Pinging 20.1.1.2 with 32 bytes of data:

Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 20.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

# Enter the IP address of Switch B in the address bar of the browser on the host. The browser can display the Web login page. Enter the username and password on the page, and the click **Login**. After login, you can perform device configuration on the associated pages.

Figure 3 Web login page of Switch B


English
H3C
Username
Password
Keep me signed in
Login
Copyright© 2004-2020 New H3C Technologies Co., Ltd. All Rights Reserved

Configuration files

- Switch A:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch B:

```
#
vlan 200
```

```
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 ip route-static 10.1.1.0 24 20.1.1.1
#
local-user admin class manage
 password hash
$h$6$BdqhpnjJwOBmHmmt$rQ/FQ6WnS9gVhEpdZY3hjvWSYxCtI+9ngtivuAwrvFdCDVE8AepcSxtprJR
5XAdrYbXQE76FumgUszLRn03a0g==
 service-type http
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
#
```

Related documentation

- Static routing configuration in the Layer 3—IP routing configuration guide for the device.
- Static routing commands in the Layer 3—IP routing command reference for the device.
- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.

Configuring basic IPv6 static route settings

Introduction

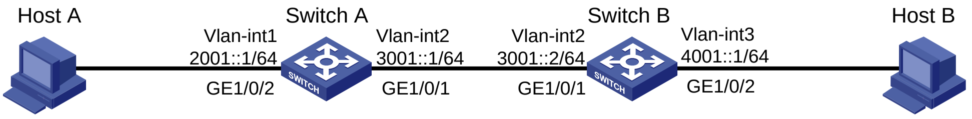
The following example describes the basic procedure to configure basic IPv6 static route settings.

Network configuration

As shown in Figure 4, the switches act as gateways of an enterprise, and they are required to perform stateless address autoconfiguration for Host A and Host B. Then the hosts in different subnets can access each other through IPv6 static routes. To meet the requirements, configure the associated settings as follows:

- Connect Host A, Host B, Switch A, and Switch B through Ethernet ports. Add the Ethernet ports to corresponding VLANs. Configure IPv6 addresses for the VLAN interfaces and verify that they are connected.
- Configure IPv6 static routes on Switch A and Switch B for interconnections between the subnets.

Figure 4 Network diagram



Procedure

Configuring Switch A

# Create VLANs and assign ports to them.

```
<SwitchA> system-view
[SwitchA] vlan 1
[SwitchA-vlan1] port gigabitethernet 1/0/2
[SwitchA-vlan1] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
```

# Specify a global unicast address for VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
```

```
[SwitchA-Vlan-interface2] quit
```

# Specify a global unicast address for VLAN-interface 1, and allow it to advertise RA messages (no interface advertises RA messages by default).

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
[SwitchA-Vlan-interface1] quit
```

# Configure an IPv6 static route with destination IPv6 address 4001::/64 and next hop address 3001::2.

```
[SwitchA] ipv6 route-static 4001:: 64 3001::2
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
```

# Specify a global unicast address for VLAN-interface 2.

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

# Specify a global unicast address for VLAN-interface 3, and allow it to advertise RA messages (no interface advertises RA messages by default).

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 4001::1/64
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
[SwitchB-Vlan-interface3] quit
```

# Configure an IPv6 static route with destination IPv6 address 2001::/64 and next hop address 3001::1.

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

Configuring Host A

Enable IPv6 for the host to automatically obtain an IPv6 address through IPv6 ND.

Configuring Host B

Enable IPv6 for the host to automatically obtain an IPv6 address through IPv6 ND.

Verifying the configuration

# Display neighbor information for GigabitEthernet 1/0/2 on Switch A.

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
2001::15B:E0EA:3524:E791  0015-e9a6-7d14 1          GE1/0/2       REACH D  1248
FE80::215:E9FF:FEA6:7D14  0015-e9a6-7d14 1          GE1/0/2       REACH D  1238
```

The output shows that the IPv6 global unicast address that Host A obtained is 2001::15B:E0EA:3524:E791.

# Display neighbor information for GigabitEthernet 1/0/2 on Switch B.

```
[SwitchB] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
4001::B15F:BC63:DBCE:EB57 6805-ca8b-18f3 3          GE1/0/2       REACH D  46
FE80::510B:D60F:31A7:4AFF 6805-ca8b-18f3 3          GE1/0/2       REACH D  1238
```

The output shows that the IPv6 global unicast address that Host B obtained is 4001::B15F:BC63:DBCE:EB57.

# Ping Host B on Switch A to verify that they are connected.

```
[Switch A] ping ipv6 4001::B15F:BC63:DBCE:EB57
Ping6(56 data bytes) 3001::1 --> 4001::B15F:BC63:DBCE:EB57, press CTRL+C to break
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=0 hlim=64 time=1.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 4001::B15F:BC63:DBCE:EB57 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

# Ping Host A on Switch B to verify that they are connected.

```
[Switch B] ping ipv6 2001::15B:E0EA:3524:E791
Ping6(56 data bytes) 3001::2 --> 2001::15B:E0EA:3524:E791, press CTRL+C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=1.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

The output shows that Host A can also ping Host B.

Configuration files

- Switch A:

```
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ipv6 address 2001::1/64
 undo ipv6 nd ra halt
#
interface Vlan-interface2
 ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1
#
 ipv6 route-static 4001:: 64 3001::2
#
```

- Switch B:

```
#
vlan 2
#
vlan 3
#
interface Vlan-interface2
 ipv6 address 3001::2/64
#
interface Vlan-interface3
 ipv6 address 4001::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 ipv6 route-static 2001:: 64 3001::1
 #
```

Related documentation

- IPv6 basics configuration in the Layer 3—IP services configuration guide for the device.
- IPv6 basics commands in the Layer 3—IP services command reference for the device.
- IPv6 static routing configuration in the Layer 3—IP routing configuration guide for the device.
- IPv6 static routing commands in the Layer 3—IP routing command reference for the device.

# Configuring a default route

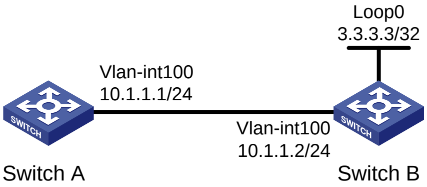
Introduction

The following information uses an example to describe the basic procedure for configuring a default route.

Network configuration

As shown in Figure 5, configure a default route on Switch A, and specify the next hop address as 10.1.1.2/24, an IP address of the interface on Switch B . After configuration, Switch A can ping loopback interface address 3.3.3.3/32 of Switch B.

Figure 5 Network diagram



Procedure

Configuring Switch A

# Create a VLAN and assign a port to it. Configure the IP address of the VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

# Configuring a default route.

```
[SwitchA] ip route-static 0.0.0.0 0 10.1.1.2
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create a VLAN and assign a port to it. Configure the IP address of the VLAN interface.

```
<SwitchB> system-view
[SwitchB] vlan 100
```

```
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
```

# Assign an IP address to the loopback interface..

```
[SwitchB] interface LoopBack 0
[SwitchB-LoopBack0] ip address 3.3.3.3 32
```

# Save the configuration.

```
[SwitchB] save force
```

Verifying the configuration

# Ping 3.3.3.3 on Switch A without a default route configured. The loopback interface address cannot be pinged.

```
[SwitchA] ping 3.3.3.3
Ping 3.3.3.3 (3.3.3.3): 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 3.3.3.3 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

# Ping 3.3.3.3 on Switch A when a default is configured. The loopback interface address can be pinged.

```
[SwitchA] ping 3.3.3.3
Ping 3.3.3.3 (3.3.3.3): 56 data bytes, press CTRL+C to break
56 bytes from 3.3.3.3: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 3.3.3.3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/2.000/0.800 ms
```

Configuration files

- Switch A:

  ```
  #
  vlan 100
  ```

```
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 ip route-static 0.0.0.0 0 10.1.1.2
#
```

- Switch B:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
```

Related documentation

- Static routing configuration in the Layer 3—IP routing configuration guide for the device.
- Static routing commands in the Layer 3—IP routing command reference for the device.

Configuring basic static route settings

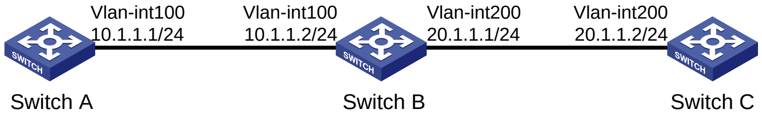
Introduction

The following information uses an example to describe the basic procedure for configuring basic static route settings.

Network configuration

As shown in Figure 6, configure static routes so that Switch A and Switch C can communicate with each other.

Figure 6 Network diagram



Procedure

Configuring Switch A

# Create a VLAN and assign a port to it. Configure the IP address of the VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

# Configure a static route.

```
[SwitchA] ip route-static 20.1.1.0 24 10.1.1.2
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them. Configure the IP addresses of the VLAN interfaces.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] vlan 200
```

```
[SwitchB-vlan200] port gigabitethernet 1/0/2
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ip address 20.1.1.1 24
[SwitchB-Vlan-interface200] quit
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring Switch C

# Create a VLAN and assign a port to it. Configure the IP address of the VLAN interface.

```
<SwitchC> system-view
[SwitchC] vlan 200
[SwitchC-vlan200] port gigabitethernet 1/0/1
[SwitchC-vlan200] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ip address 20.1.1.2 24
[SwitchC-Vlan-interface200] quit
```

# Configure a static route.

```
[SwitchC] ip route-static 10.1.1.0 24 20.1.1.1
```

# Save the configuration.

```
[SwitchC] save force
```

Verifying the configuration

# Ping Switch C on Switch A to verify that they are connected.

```
[SwitchA] ping 20.1.1.2
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=2.000 ms
56 bytes from 20.1.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 20.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 20.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 20.1.1.2: icmp_seq=4 ttl=255 time=0.000 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 = 0.000/0.600/2.000/0.800 ms
```

Configuration files

- Switch A:

  ```
  #
  vlan 100
  ```

```
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 ip route-static 20.1.1.0 24 10.1.1.2
#
```

- Switch B:

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch C:

```
#
vlan 200
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 ip route-static 10.1.1.0 24 20.1.1.1
#
```

Related documentation

- Static routing configuration in the Layer 3—IP routing configuration guide for the device.

- Static routing commands in the Layer 3—IP routing command reference for the device.

Configuring a floating static route

Introduction

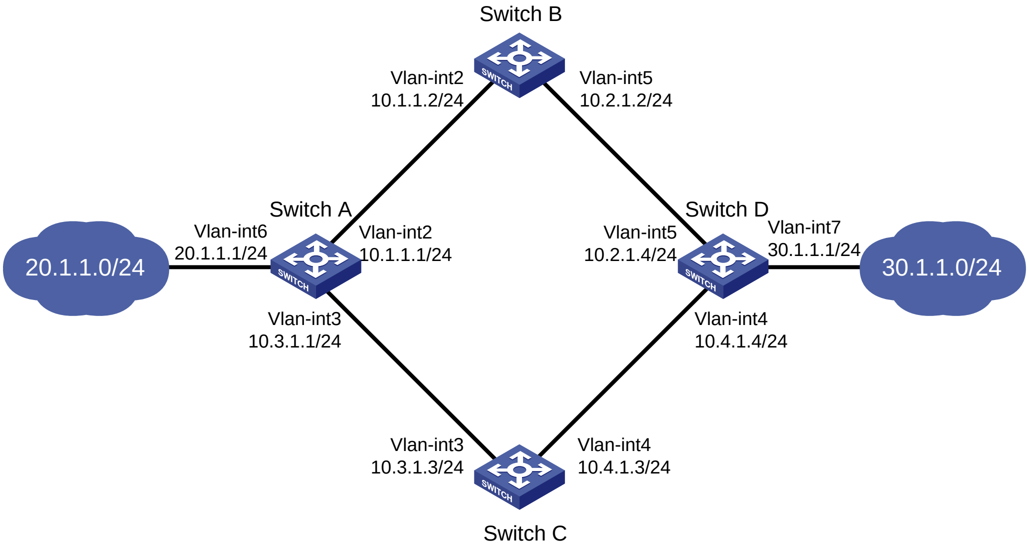
The following information uses an example to describe the basic procedure for configuring a floating static route.

Network configuration

A floating static route is used for route backup. As shown in Figure 7, Switch A is the default gateway of the hosts in network 20.1.1.0/24. To ensure network availability, configure static routes to 30.1.1.0/24 (attached to Switch D) for backup on Switch A as follows:

- The static route with next hop Switch B acts as the master route.
- The static route with next hop Switch C acts as the backup route. When the master route is unavailable, the backup route takes effect. Switch A forwards packets to 30.1.1.0/24 through Switch C.
- When the master route recovers, service traffic switches back to the master route.

Figure 7 Network diagram



Procedure

Configuring Switch A

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 6
[SwitchA-vlan6] port gigabitethernet 1/0/3
[SwitchA-vlan6] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.3.1.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 20.1.1.1 24
[SwitchA-Vlan-interface6] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.1.1.2 and the default priority (60).

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2
```

# Configure a static route to 30.1.1.0/24 with next hop 10.3.1.3 and priority 80.

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 24
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 10.2.1.2 24
[SwitchB-Vlan-interface5] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.2.1.4.

```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

# Configure a static route to 20.1.1.0/24 with next hop 10.1.1.1.

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring Switch C

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] quit
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/2
[SwitchC-vlan4] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 10.3.1.3 24
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 10.4.1.3 24
[SwitchC-Vlan-interface4] quit
```

# Configure a static route to 30.1.1.0/24 with next hop 10.4.1.4.

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

# Configure a static route to 20.1.1.0/24 with next hop 10.3.1.1.

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

# Save the configuration.

```
[SwitchC] save force
```

Configuring Switch D

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchD> system-view
[SwitchD] vlan 4
[SwitchD-vlan4] port gigabitethernet 1/0/1
[SwitchD-vlan4] quit
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/2
[SwitchD-vlan5] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface6] ip address 10.4.1.4 24
[SwitchD-Vlan-interface6] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 10.2.1.4 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 30.1.1.1 24
[SwitchD-Vlan-interface7] quit
```

# Configure a static route to 20.1.1.0/24 with next hop 10.2.1.2 and the default priority (60).

```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2
```

# Configure a static route to 20.1.1.0/24 with next hop 10.4.1.3 and priority 80.

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

# Save the configuration.

```
[SwitchD] save force
```

Verifying the configuration

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table

Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
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
```

The output shows that Switch A forwards packets to 30.1.1.0/24 through Switch B.

# Remove the IP address of interface VLAN-interface 2 on Switch B.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] undo ip address
```

# Display the routing table of Switch A.

```
[SwitchA] display ip routing-table

Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
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
```

The output shows that Switch A forwards packets to 30.1.1.0/24 through Switch B. The backup route takes effect.

# Verify that hosts in 20.1.1.0/24 can communicate with the hosts in 30.1.1.0/24 when the master route fails.

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

# Verify associated information on Switch D (similar to that on Switch A). Verify that hosts in 30.1.1.0/24 can communicate with the hosts in 20.1.1.0/24 when the master route fails.

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Configuration files

- Switch A:

```
#
vlan 2
#
vlan 3
#
vlan 6
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface6
```

```
 ip address 20.1.1.1 255.255.255.0
#
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 access vlan 6
#
 ip route-static 30.1.1.0 24 10.1.1.2
 ip route-static 30.1.1.0 24 10.3.1.3 preference 80
#
```

- Switch B:

```
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 20.1.1.0 24 10.1.1.1
 ip route-static 30.1.1.0 24 10.2.1.4
#
```

- Switch C:

```
#
vlan 3
#
vlan 4
#
interface Vlan-interface3
 ip address 10.3.1.3 255.255.255.0
```

```
#
interface Vlan-interface4
 ip address 10.4.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.4
#
```

- Switch D:

```
#
vlan 4
#
vlan 5
#
vlan 7
#
interface Vlan-interface4
 ip address 10.4.1.4 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.4 255.255.255.0
#
interface Vlan-interface7
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
#
 ip route-static 20.1.1.0 24 10.2.1.2
 ip route-static 20.1.1.0 24 10.4.1.3 preference 80
#
```

Related documentation

- Static routing configuration in the Layer 3—IP routing configuration guide for the device.
- Static routing commands in the Layer 3—IP routing command reference for the device.

Basic RIP Quick Start Configuration Guide

Contents

Configuring basic RIP settings 1

Introduction 1

Network configuration 1

Procedure 1

Verifying the configuration 3

Configuration files 4

Related documentation 6

Configuring basic RIP settings

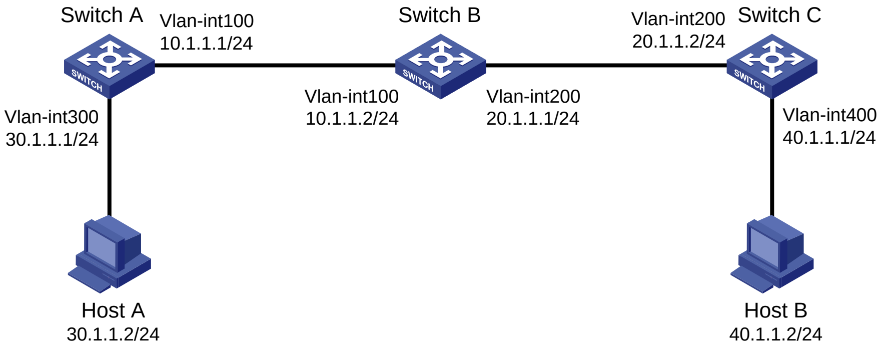
Introduction

The following information uses an example to describe the basic procedure for configuring basic RIP settings.

Network configuration

As shown in Figure 1, enable RIPv2 on all switches so that Host A and Host B can communicate with each other.

Figure 1 Network diagram



Procedure

Configuring Host A and Host B

# Configure IP address 30.1.1.2, subnet mask 255.255.255.0, and gateway address 30.1.1.1 for Host A. (Details not shown.)

# Configure IP address 40.1.1.2, subnet mask 255.255.255.0, and gateway address 40.1.1.1 for Host B. (Details not shown.)

Configuring Switch A

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 300
[SwitchA-vlan300] port gigabitethernet 1/0/2
```

```
[SwitchA-vlan300] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ip address 30.1.1.1 24
[SwitchA-Vlan-interface300] quit
```

# Configure RIPv2 settings.

```
[SwitchA] rip
[SwitchA-rip-1] network 10.1.1.0
[SwitchA-rip-1] network 30.1.1.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] vlan 200
[SwitchB-vlan200] port gigabitethernet 1/0/2
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ip address 20.1.1.1 24
[SwitchB-Vlan-interface200] quit
```

# Configure RIPv2 settings.

```
[SwitchB] rip
[SwitchB-rip-1] network 10.1.1.0
[SwitchB-rip-1] network 20.1.1.0
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] quit
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring Switch C

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchC> system-view
[SwitchC] vlan 200
```

```
[SwitchC-vlan200] port gigabitethernet 1/0/1
[SwitchC-vlan200] quit
[SwitchC] vlan 400
[SwitchC-vlan400] port gigabitethernet 1/0/2
[SwitchC-vlan400] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ip address 20.1.1.2 24
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ip address 40.1.1.1 24
[SwitchC-Vlan-interface400] quit
```

# Configure RIPv2 settings.

```
[SwitchC] rip
[SwitchC-rip-1] network 20.1.1.0
[SwitchC-rip-1] network 40.1.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] quit
```

# Save the configuration.

```
[SwitchC] save force
```

Verifying the configuration

# Display the RIP routing table of Switch A.

```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------------------
 Peer 10.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop         Cost    Tag     Flags   Sec
      20.1.1.0/24             10.1.1.2        1       0       RAOF    27
      40.1.1.0/24             10.1.1.2        2       0       RAOF    27
 Local route
      Destination/Mask        Nexthop         Cost    Tag     Flags   Sec
      10.1.1.0/24             0.0.0.0         0       0       RDOF    -
      30.1.1.0/24             0.0.0.0         0       0       RDOF    -
```

# Display the RIP routing table of Switch B.

```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------------------
 Peer 10.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop         Cost    Tag     Flags   Sec
      30.1.1.0/24             10.1.1.1        1       0       RAOF    0
 Peer 20.1.1.2 on Vlan-interface200
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      40.1.1.0/24             20.1.1.2          1       0       RAOF    9
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      20.1.1.0/24             0.0.0.0           0       0       RDOF    -
      10.1.1.0/24             0.0.0.0           0       0       RDOF    -
```

# Display the RIP routing table of Switch C.

```
[SwitchC] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ----------------------------------------------------------------------------
 Peer 20.1.1.1 on Vlan-interface200
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      10.1.1.0/24             20.1.1.1          1       0       RAOF    32
      30.1.1.0/24             20.1.1.1          2       0       RAOF    32
 Local route
      Destination/Mask        Nexthop           Cost    Tag     Flags   Sec
      20.1.1.0/24             0.0.0.0           0       0       RDOF    -
      40.1.1.0/24             0.0.0.0           0       0       RDOF    -
```

# Ping Host B on Host A to verify that Host B is reachable (assuming Windows XP is installed on the host).

```
C:\Documents and Settings\Administrator>ping 40.1.1.2

Pinging 40.1.1.2 with 32 bytes of data:

Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 40.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Configuration files

- Switch A:

```
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
 network 30.0.0.0
```

```
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 300
#
```

- Switch B:

```
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
 network 20.0.0.0
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch C:

```
#
rip 1
```

```
 undo summary
 version 2
 network 20.0.0.0
 network 40.0.0.0
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface400
 ip address 40.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 400
#
```

Related documentation

- RIP configuration in the Layer 3—IP routing configuration guide for the device.
- RIP commands in the Layer 3—IP routing command reference for the device.

PBR Quick Start Configuration Guide

Contents

Configuring source-IP-based interface PBR ······························ 1

Introduction ······························ 1

Network configuration ······························ 1

Procedure ······························ 2

Verifying the configuration ······························ 5

Configuration files ······························ 6

Related documentation ······························ 9

Configuring source-IP-based interface PBR

Introduction

The following information uses an example to describe the basic procedure for configuring source-IP-based interface PBR.

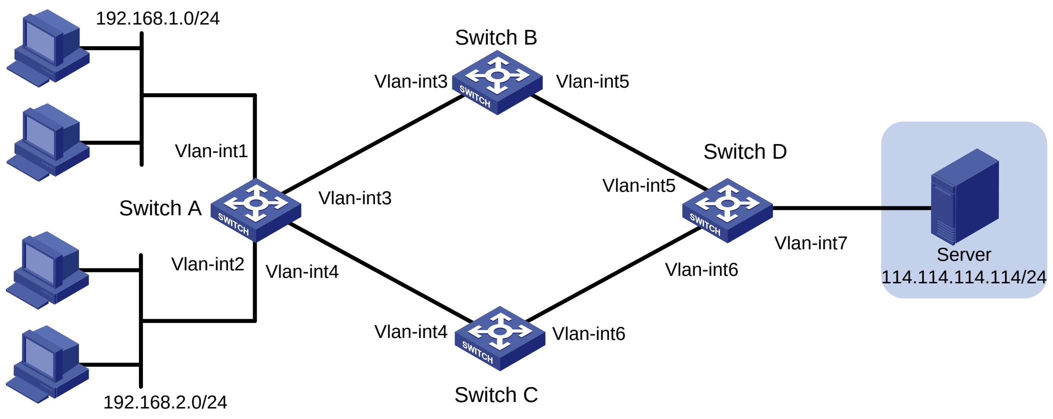
Network configuration

As shown in Figure 1, Configure static routes so that Switch A can forward all packets destined to the server (114.114.114.114/24) through Switch B.

Configure interface PBR to guide the forwarding of packets destined to the 114.114.114.114/24 received on VLAN-interface 2 of Switch A as follows:

- Set the next hop of packets sourced from 192.168.2.0/24 to Switch C.
- Set the next hop of other packets to Switch B.

Figure 1 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int1	192.168.1.1/24	Switch C:	Vlan-int4	20.20.20.2/24
	Vlan-int2	192.168.2.1/24		Vlan-int6	40.40.40.1/24
	Vlan-int3	10.10.10.1/24	Switch D:	Vlan-int5	30.30.30.2/24
	Vlan-int4	20.20.20.1/24		Vlan-int6	40.40.40.2/24
Switch B:	Vlan-int3	10.10.10.2/24		Vlan-int7	114.114.114.1/24
	Vlan-int5	30.30.30.1/24			

Procedure

Configuring Host A and Host B

# Configure IP address 192.168.1.2, subnet mask 255.255.255.0, and gateway address 192.168.1.1 for Host A. (Details not shown.)

# Configure IP address 192.168.2.2, subnet mask 255.255.255.0, and gateway address 192.168.2.1 for Host B. (Details not shown.)

Configuring Switch A

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchA> system-view
[SwitchA] vlan 1
[SwitchA-vlan1] port gigabitethernet 1/0/1
[SwitchA-vlan1] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/3
[SwitchA-vlan3] quit
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/4
[SwitchA-vlan4] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.1.1 24
[SwitchA-Vlan-interface1] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.2.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.10.10.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.20.20.1 24
[SwitchA-Vlan-interface4] quit
```

# Configure a static route with destination address 114.114.114.114/24. Without PBR configured, all packets destined to 114.114.114.114/24 are forwarded through Switch B.

```
[SwitchA] ip route-static 114.114.114.114 24 10.10.10.2
```

# Configure ACL 3000 to match packets sourced from 192.168.2.0/24.

```
[SwitchA] acl advanced 3000
[SwitchA-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255
[SwitchA-acl-ipv4-adv-3000] quit
```

# Configure ACL 3001 to match packets sourced from 192.168.2.0/24 and destined to 192.168.1.0/24.

```
[SwitchA] acl advanced 3001
[SwitchA-acl-ipv4-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination 
192.168.1.0 0.0.0.255
[SwitchA-acl-ipv4-adv-3001] quit
```

# Configure Node 10 for the policy **aaa** and specify ACL 3001 for the policy node. Do not specify any apply clauses for the policy node to avoid interrupting traffic between different interfaces on Switch A. (Matching packets will be forwarded according to routing table lookup, and the next node will not be matched. This configuration ensures forwarding of packets between different subnets in the internal network without being processed by PBR. By default, the gateways on different subnets can access one another.

```
[SwitchA] policy-based-route aaa permit node 10
[SwitchA-pbr-aaa-10] if-match acl 3001
[SwitchA-pbr-aaa-10] quit
```

# Configure Node 20 for the policy **aaa** to forward packets matching ACL 3000 to next hop 20.20.20.2.

```
[SwitchA] policy-based-route aaa permit node 20
[SwitchA-pbr-aaa-20] if-match acl 3000
[SwitchA-pbr-aaa-20] apply next-hop 20.20.20.2
[SwitchA-pbr-aaa-20] quit
```

# Configure interface PBR by applying policy **aaa** to VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip policy-based-route aaa
[SwitchA-Vlan-interface2] quit
```

# Enable sending ICMP destination unreachable messages.

```
[SwitchA] ip unreachables enable
```

# Enable sending ICMP time exceeded messages.

```
[SwitchA] ip ttl-expires enable
```

# Save the configuration.

```
[SwitchA] save force
```

Configuring Switch B

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 10.10.10.2 24
[SwitchB-Vlan-interface3] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 30.30.30.1 24
```

```
[SwitchB-Vlan-interface5] quit
```

# Configure a static route with destination address 114.114.114.114/32.

```
[SwitchB] ip route-static 114.114.114.114 24 30.30.30.2
```

# Configure a static route with destination address 192.168.1.0/24.

```
[SwitchB] ip route-static 192.168.1.0 24 10.10.10.1
```

# Configure a static route with destination address 192.168.2.0/24.

```
[SwitchB] ip route-static 192.168.2.0 24 10.10.10.1
```

# Enable sending ICMP destination unreachable messages.

```
[SwitchB] ip unreachables enable
```

# Enable sending ICMP time exceeded messages.

```
[SwitchB] ip ttl-expires enable
```

# Save the configuration.

```
[SwitchB] save force
```

Configuring Switch C

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchC> system-view
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/1
[SwitchC-vlan4] quit
[SwitchC] vlan 6
[SwitchC-vlan6] port gigabitethernet 1/0/2
[SwitchC-vlan6] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 20.20.20.2 24
[SwitchC-Vlan-interface4] quit
[SwitchC] interface vlan-interface 6
[SwitchC-Vlan-interface6] ip address 40.40.40.1 24
[SwitchC-Vlan-interface6] quit
```

# Configure a static route with destination address 114.114.114.114/32.

```
[SwitchC] ip route-static 114.114.114.114 24 40.40.40.2
```

# Configure a static route with destination address 192.168.1.0/24.

```
[SwitchC] ip route-static 192.168.1.0 24 20.20.20.1
```

# Configure a static route with destination address 192.168.2.0/24.

```
[SwitchC] ip route-static 192.168.2.0 24 20.20.20.1
```

# Enable sending ICMP destination unreachable messages.

```
[SwitchC] ip unreachables enable
```

# Enable sending ICMP time exceeded messages.

```
[SwitchC] ip ttl-expires enable
```

# Save the configuration.

```
[SwitchC] save force
```

Configuring Switch D

# Create VLANs and assign ports to them. Configure the IP address of each VLAN interface.

```
<SwitchD> system-view
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/1
[SwitchD-vlan5] quit
[SwitchD] vlan 6
[SwitchD-vlan6] port gigabitethernet 1/0/2
[SwitchD-vlan6] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 30.30.30.2 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 6
[SwitchD-Vlan-interface6] ip address 40.40.40.2 24
[SwitchD-Vlan-interface6] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 114.114.114.1 24
[SwitchD-Vlan-interface7] quit
```

# Configure a static route with destination address 192.168.1.0/24.

```
[SwitchD] ip route-static 192.168.1.0 24 30.30.30.1
```

# Configure a static route with destination address 192.168.2.0/24.

```
[SwitchD] ip route-static 192.168.2.0 24 40.40.40.1
```

# Enable sending ICMP destination unreachable messages.

```
[SwitchD] ip unreachables enable
```

# Enable sending ICMP time exceeded messages.

```
[SwitchD] ip ttl-expires enable
```

# Save the configuration.

```
[SwitchD] save force
```

Verifying the configuration

# Execute the **display ip policy-based-route** command on Switch A to verify that interface PBR is successfully configured.

```
[SwitchA] display ip policy-based-route interface Vlan-interface 2
Policy-based routing information for interface Vlan-interface2:
Policy name: aaa
  node 10 permit:
    if-match acl 3001
  Matches: 0, bytes: 0
  node 20 permit:
    if-match acl 3000
    apply next-hop 20.20.20.2
  Matches: 0, bytes: 0
Total matches: 0, total bytes: 0
```

# Use the **`tracert`** command to identify the path from Host A to the server 114.114.114.114/24. (To use the tracert function, enable sending ICMP time exceeded messages on intermediate devices, and enable sending ICMP destination unreachable messages on the destination device.) You can see that the packets are forwarded through Switch B.

```
C:\Documents and Settings\Administrator>tracert 114.114.114.114

Tracing route to 114.114.114.114 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    <1 ms    <1 ms    <1 ms  10.10.10.2
  3    <1 ms    <1 ms    <1 ms  30.30.30.2
  4     1 ms    <1 ms    <1 ms  114.114.114.114

Trace complete.
```

# Use the **`tracert`** command to identify the path from Host B to the server 114.114.114.114/24. You can see that the packets are forwarded through Switch C. The PBR configuration has taken effect.

```
C:\Documents and Settings\Administrator>tracert 114.114.114.114

Tracing route to 114.114.114.114 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2    <1 ms    <1 ms    <1 ms  20.20.20.2
  3    <1 ms    <1 ms    <1 ms  40.40.40.2
  4     1 ms    <1 ms    <1 ms  114.114.114.114

Trace complete.
```

Configuration files

- Switch A:

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 1
#
vlan 2 to 4
#
policy-based-route aaa permit node 10
 if-match acl 3001
#
policy-based-route aaa permit node 20
 if-match acl 3000
 apply next-hop 20.20.20.2
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
 ip policy-based-route aaa
#
interface Vlan-interface3
 ip address 10.10.10.1 255.255.255.0
#
interface Vlan-interface4
 ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
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 access vlan 4
#
 ip route-static 114.114.114.114 24 10.10.10.2
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
```

- Switch B:

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 3
#
vlan 5
#
interface Vlan-interface3
```

```
 ip address 10.10.10.2 255.255.255.0
#
interface Vlan-interface5
 ip address 30.30.30.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 114.114.114.114 24 30.30.30.2
 ip route-static 192.168.1.0 24 10.10.10.1
 ip route-static 192.168.2.0 24 10.10.10.1
#
```

- Switch C:

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 4
#
vlan 6
#
interface Vlan-interface4
 ip address 20.20.20.2 255.255.255.0
#
interface Vlan-interface6
 ip address 40.40.40.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 6
#
 ip route-static 114.114.114.114 24 40.40.40.2
 ip route-static 192.168.1.0 24 20.20.20.1
 ip route-static 192.168.2.0 24 20.20.20.1
#
```

- Switch D:

```
#
 ip unreachables enable
 ip ttl-expires enable
```

```
#
vlan 5 to 7
#
interface Vlan-interface5
 ip address 30.30.30.2 255.255.255.0
#
interface Vlan-interface6
 ip address 40.40.40.2 255.255.255.0
#
interface Vlan-interface7
 ip address 114.114.114.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
#
 ip route-static 192.168.1.0 24 30.30.30.1
 ip route-static 192.168.2.0 24 40.40.40.1
#
```

Related documentation

- Policy-based routing configuration in the Layer 3—IP routing configuration guide for the device.
- Policy-based routing commands in the Layer 3—IP routing command reference for the device.

IGMP snooping Quick Start Configuration Guide

Contents

Configuring IGMP snooping ······························· 1

Introduction ······························· 1
Network configuration ······························· 1
Procedure······························· 1
Verify the configuration ······························· 2
Configuration files ······························· 2
Related documentation ······························· 3

Configuring IGMP snooping

Introduction

The following information uses an example to describe the basic procedure for configuring IGMP snooping.

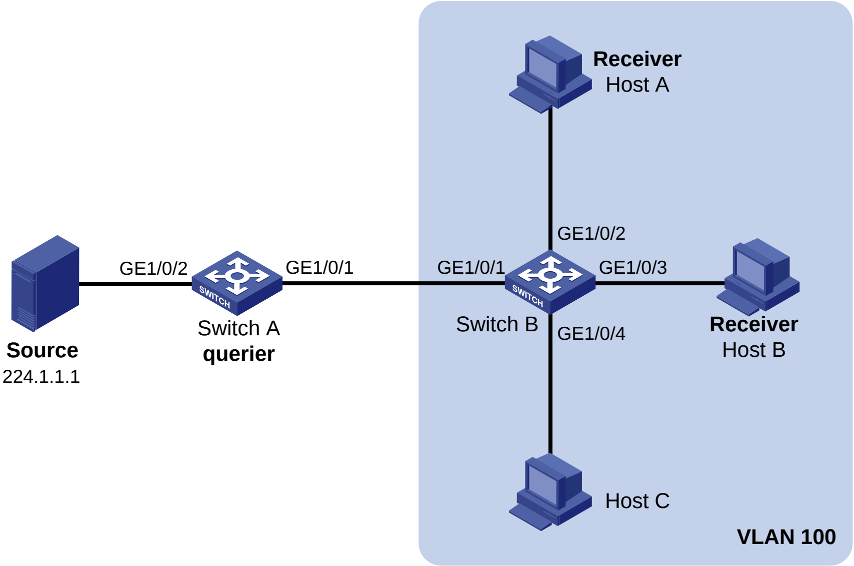
Network configuration

As shown in Figure 1:

- The network is a Layer 2-only network.
- The multicast source sends multicast data to multicast group 224.1.1.1.
- Host A and Host B are receivers of multicast group 224.1.1.1, and Host C is not a receiver of multicast group 224.1.1.1.
- All host receivers run IGMPv2, and all switches run IGMPv2 snooping. Switch A (which is close to the multicast sources) acts as the IGMP snooping querier.

To send multicast data only to Host A and Host B in the Layer 2-only network, enable IGMP snooping on Switch B.

Figure 1 Network diagram



Procedure

Configuring Switch A

# Enable the IGMP snooping feature.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/2 to the VLAN, enable IGMP snooping for VLAN 100.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[SwitchA-vlan100] igmp-snooping enable
```

# Configure Switch A as the IGMP snooping querier.

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

# Set the configuration.

```
[SwitchA] save
```

Configuring Switch B

# Enable the IGMP snooping feature.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

# Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN, enable IGMP snooping for VLAN 100.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

Verify the configuration

# Display dynamic IGMP snooping group entries on Switch B.

```
<SwitchB> display igmp-snooping group
Total 2 entries.

VLAN 100: Total 2 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/2                           (00:03:23)
      GE1/0/3                           (00:03:23)
```

The output shows that GE1/0/4 of Host C is not in the multicast group. Multicast data is not sent to Host.

Configuration files

- Switch A:

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
 igmp-snooping querier
#
interface GigabitEthernet1/0/1
```

```
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
```

- Switch B:

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

Related documentation

- IGMP snooping configuration in the IP multicast configuration guide for the device.
- IGMP snooping commands in the IP multicast command reference for the device.

Packet Filtering Quick Start Configuration Guide

Contents

Configuring packet filtering ··· 1

Introduction ··· 1

Network configuration ··· 1

Procedure ··· 1

Verify the configuration ··· 2

Configuration files ··· 3

Related documentation ··· 3

Configuring packet filtering

Introduction

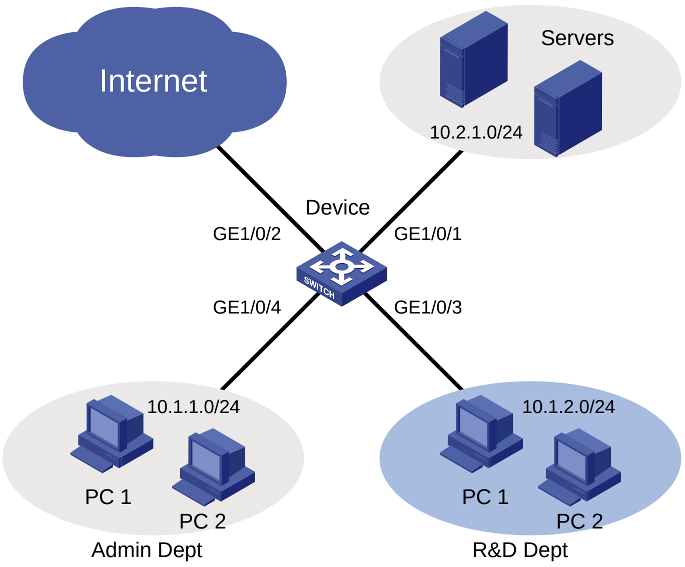
The following information uses an example to describe the basic procedure for configuring packet filtering.

Network configuration

As shown in Figure 1, a company interconnects its departments through the device. Configure packet filtering to:

- Permit access from the Admin Dept at any time to the Internet and servers and deny access from the Admin Dept to the R&D Dept.
- Permit access from the R&D Dept to the servers and deny access from the R&D Dept to the Internet and the Admin Dept.

Figure 1 Network diagram



Procedure

1. Configure access to the Admin Dept.

   # Create an IPv4 advanced ACL numbered 3000.

   ```
   <Device> system-view
   [Device] acl advanced 3000
   ```

   # Configure a rule to deny packets from the R&D Dept.

   ```
   [Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
   [Device-acl-ipv4-adv-3000] quit
   ```

   # Apply IPv4 advanced 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
```

2. Configure access to the R&D Dept.

   # Create an IPv4 advanced ACL numbered 3001.

   ```
   [Device] acl advanced 3001
   ```

   # Configure a rule to permit packets from the Admin Dept.

   ```
   [Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255
   ```

   # Configure a rule to deny all other packets.

   ```
   [Device-acl-ipv4-adv-3001] rule deny ip
   ```

   # Apply IPv4 advanced 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
   ```

Verify the configuration

# Display ACL application information for inbound 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
```

The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 are successfully applied with ACLs for packet filtering.

# Verify that a website on the Internet cannot be pinged from a PC in the R&D Dept.

```
C:\>ping www.google.com

Pinging www.google.com [172.217.194.99] 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 a server can be pinged from a PC in the R&D Dept.

```
C:\>ping 10.2.1.10
Ping 192.168.1.60 (10.2.1.10): 56 data bytes, press CTRL+C to break
56 bytes from 10.2.1.10: icmp_seq=0 ttl=255 time=12.963 ms
56 bytes from 10.2.1.10: icmp_seq=1 ttl=255 time=4.168 ms
56 bytes from 10.2.1.10: icmp_seq=2 ttl=255 time=7.390 ms
56 bytes from 10.2.1.10: icmp_seq=3 ttl=255 time=3.363 ms
56 bytes from 10.2.1.10: icmp_seq=4 ttl=255 time=2.901 ms
C:\>
```

# Verify that a website on the Internet can be pinged from a PC in the Admin Dept.

```
C:\>ping www.google.com

Pinging www.google.com [172.217.194.99] with 32 bytes of data:

Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50

Ping statistics for 172.217.194.99:
    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 Ten-GigabitEthernet1/0/3
 port link-mode bridge
 packet-filter 3001 inbound
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 packet-filter 3000 inbound
#
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
 rule 5 deny ip
#
```

Related documentation

- ACL configuration in the ACL and QoS configuration guide for the device.
- ACL commands in the ACL and QoS command reference for the device.

QoS Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring IP rate limiting ··· 1

Introduction ··· 1
Network configuration ··· 1
Analysis ··· 1
Procedure ··· 2
Verify the configuration ··· 3
Configuration files ··· 4
Related documentation ··· 5

Configuring class-based accounting ··· 6

Introduction ··· 6
Network configuration ··· 6
Procedure ··· 6
Verify the configuration ··· 7
Configuration files ··· 8
Related documentation ··· 9

Configuring IP rate limiting

Introduction

The following information uses an example to describe the basic procedure for configuring IP 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.

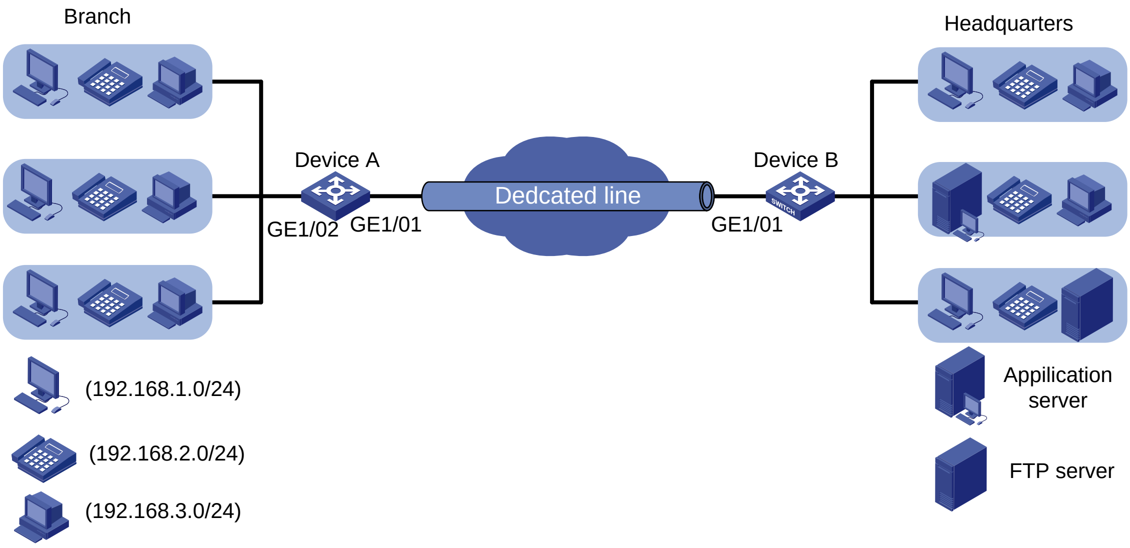
The following traffic policing settings have been configured on the edge device (Device B) of the headquarters:

- 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 (Device A) of the branch to buffer excess traffic of each traffic type.

Configure rate limiting on Device 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.

Procedure

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).

   ```
   <DeviceA> system-view
   [DeviceA] acl basic 2000
   [DeviceA-acl-ipv4-basic-2000] rule permit source 192.168.3.0 0.0.0.255
   [DeviceA-acl-ipv4-basic-2000] quit
   ```

   # Create a class named **voice**, and use ACL 2000 as the match criterion.

   ```
   [DeviceA] traffic classifier voice
   [DeviceA-classifier-voice] if-match acl 2000
   [DeviceA-classifier-voice] quit
   ```

   # Configure basic IPv4 ACL 2001 to match application traffic (traffic from subnet 192.168.2.0/24).

   ```
   [DeviceA] acl basic 2001
   [DeviceA-acl-ipv4-basic-2001] rule permit source 192.168.2.0 0.0.0.255
   [DeviceA-acl-ipv4-basic-2001] quit
   ```

   # Create a class named **service**, and use ACL 2001 as the match criterion.

   ```
   [DeviceA] traffic classifier service
   [DeviceA-classifier-service] if-match acl 2001
   [DeviceA-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).

   ```
   [DeviceA] acl advanced 3000
   [DeviceA-acl-ipv4-adv-3000] rule permit tcp destination-port eq 20 source 192.168.1.0
   0.0.0.255
   [DeviceA-acl-ipv4-adv-3000] quit
   ```

   # Create a class named **ftp**, and use ACL 3000 as the match criterion.

   ```
   [DeviceA] traffic classifier ftp
   [DeviceA-classifier-ftp] if-match acl 3000
   [DeviceA-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).

   ```
   [DeviceA] traffic behavior voice
   [DeviceA-behavior-voice] remark local-precedence 6
   [DeviceA-behavior-voice] quit
   ```

   # Create a behavior named **service**, and configure the behavior to mark packets with local precedence 4 (corresponding to queue 4).

   ```
   [DeviceA] traffic behavior service
   ```

```
[DeviceA-behavior-service] remark local-precedence 4
[DeviceA-behavior-service] quit
```

# Create a behavior named **ftp**, and configure the behavior to mark packets with local precedence 2 (corresponding to queue 2).

```
[DeviceA] traffic behavior ftp
[DeviceA-behavior-ftp] remark local-precedence 2
[DeviceA-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.

```
[DeviceA] qos policy shaping
[DeviceA-qospolicy-shaping] classifier voice behavior voice
[DeviceA-qospolicy-shaping] classifier service behavior service
[DeviceA-qospolicy-shaping] classifier ftp behavior ftp
[DeviceA-qospolicy-shaping] quit
```

# Apply the QoS policy **shaping** to the inbound direction of GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] qos apply policy shaping inbound
[DeviceA-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).

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-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).

```
[DeviceA-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).

```
[DeviceA-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.

```
[DeviceA-GigabitEthernet1/0/1] qos lr outbound cir 15360
```

Verify the configuration

# Display ACL application information for inbound packet filtering.

# Verify the priority marking settings of GigabitEthernet 1/0/2.

```
<Device> 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.

```
<Device> 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.

```
<Device> 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
```

Related documentation

- ACL configuration in the ACL and QoS configuration guide for the device.
- ACL commands in the ACL and QoS command reference for the device.

Configuring class-based accounting

Introduction

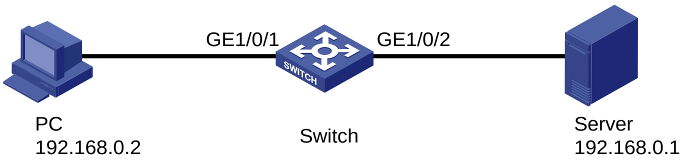
The following information uses an example to describe the basic procedure for configuring class-based accounting.

Network configuration

As shown in Figure 1, packet loss occurs when the PC accesses the server.

Configure class-based accounting through a QoS policy on the switch to check whether the packets are dropped by the switch.

Figure 2 Network diagram



Procedure

# Create advance IPv4 ACL 3001, configure a rule to match the packets with source IP address 192.168.0.2 and destination IP address 192.168.0.1, and configure another rule to match the packets with source IP address 192.168.0.1 and destination IP address 192.168.0.2.

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule 0 permit ip source 192.168.0.2 0 destination
192.168.0.241 0
[Sysname-acl-ipv4-adv-3001] rule 5 permit ip source 192.168.0.241 0 destination
192.168.0.2 0
[Sysname-acl-ipv4-adv-3001] quit
```

# Create a class named **aa**, and use ACL 3001 as the match criterion.

```
[Sysname] traffic classifier aa
[Sysname-classifier-1] if-match acl 3001
[Sysname-classifier-1] quit
```

# Create a traffic behavior named **aa**, and configure a class-based accounting action.

```
[Sysname] traffic behavior aa
[Sysname-behavior-1] accounting packet
[Sysname-behavior-1] quit
```

# Create a QoS policy named **aa**, and associate the traffic classes with the traffic behaviors in the QoS policy.

```
[Sysname] qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

# Apply the QoS policy **aa** to the inbound and outbound directions of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy 1 inbound
[Sysname-GigabitEthernet1/0/1] qos apply policy 1 outbound
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] qos apply policy 1 inbound
[Sysname-GigabitEthernet1/0/2] qos apply policy 1 outbound
[Sysname-GigabitEthernet1/0/2] quit
```

Verify the configuration

# Verify that the server can be successfully pinged from the PC.

```
C:\Users\user>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

# Verify that the switch forwards all packets from the PC.

```
[Sysname] display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
   Behavior: aa
      Accounting enable:
        4 (Packets)

Interface: GigabitEthernet1/0/1
  Direction: Outbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: aa
      Accounting enable:
        7 (Packets)
```

```
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
   Behavior: aa
      Accounting enable:
        7 (Packets)

Interface: GigabitEthernet1/0/2
  Direction: Outbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: aa
      Accounting enable:
        4 (Packets)
```

The output shows that the switch forwarded all packets from the PC (received four packets on GE 1/0/1 and sent four packets on GE 1/0/2).

Configuration files

```
#
traffic classifier aa operator and
 if-match acl 3001
#
traffic behavior aa
 accounting packet
#
qos policy aa
 classifier aa behavior aa
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos apply policy aa inbound
 qos apply policy aa outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos apply policy aa inbound
 qos apply policy aa outbound
#
acl number 3001
```

```
rule 0 permit ip source 192.168.0.2 0 destination 192.168.0.1 0
rule 5 permit ip source 192.168.0.1 0 destination 192.168.0.2 0
#
```

Related documentation

- QoS configuration in the ACL and QoS configuration guide for the device.
- QoS commands in the ACL and QoS command reference for the device.

IP Source Guard Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring static IPSG bindings ··· 1

Introduction ··· 1

Restrictions and guidelines ··· 1

Network configuration ··· 1

Procedure ··· 1

Verifying the configuration ··· 2

Configuration files ··· 3

Related documentation ··· 3

Configuring static IPSG bindings

Introduction

The following information uses an example to describe the basic procedure for configuring IP source guard (IPSG) static bindings.

Restrictions and guidelines

You cannot configure the IPSG feature on a service loopback interface or an aggregate interface.

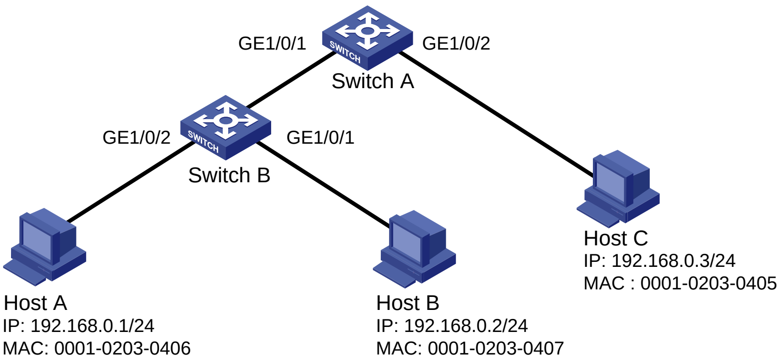
Network configuration

As shown in Figure 1, all hosts use static IP addresses.

Configure static IPv4SG bindings on Switch A and Switch B to meet the following requirements:

- GigabitEthernet 1/0/2 on Switch A allows IP packets from Host C to pass.
- GigabitEthernet 1/0/1 on Switch A allows IP packets from Host A to pass.
- GigabitEthernet 1/0/2 on Switch B allows IP packets from Host A to pass.
- GigabitEthernet 1/0/1 on Switch B allows IP packets from the host whose IP address is 192.168.0.2/24 to pass. Thus, Host B can use that IP address to reach Host A even if the MAC address of Host B changes.

Figure 1 Network diagram



Procedure

Configuring Switch A

# Enable IPv4SG on GigabitEthernet 1/0/2.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

# On GigabitEthernet 1/0/2, configure a static IPv4SG binding for Host C. (Bind the IP address and MAC address of Host C.)

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address
0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

# Enable IPv4SG on GigabitEthernet 1/0/1.

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

# On GigabitEthernet 1/0/1, configure a static IPv4SG binding for Host A. (Bind the IP address and MAC address of Host A.)

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[SwitchA-GigabitEthernet1/0/1] quit
```

# Save the configuration.

```
[SwitchA] save
```

Configuring Switch B

# Enable IPv4SG on GigabitEthernet 1/0/2.

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

# On GigabitEthernet 1/0/2, configure a static IPv4SG binding for Host A. (Bind the IP address and MAC address of Host A.)

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address
0001-0203-0406
[SwitchB-GigabitEthernet1/0/2] quit
```

# Enable IPv4SG on GigabitEthernet 1/0/1.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address
```

# On GigabitEthernet 1/0/1, configure a static IPv4SG binding for Host B. (Bind the IP address of Host B.)

```
[SwitchB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
[SwitchB-GigabitEthernet1/0/1] quit
```

# Save the configuration.

```
[SwitchB] save
```

Verifying the configuration

# Verify that the static IPv4SG bindings are configured successfully on Switch A.

```
[SwitchA] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface                VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/1                  N/A  Static
192.168.0.3     0001-0203-0405 GE1/0/2                  N/A  Static
```

# Verify that the static IPv4SG bindings are configured successfully on Switch B.

```
[SwitchB] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface                VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/2                  N/A  Static
```

```
192.168.0.2     N/A            GE1/0/1                  N/A  Static
```

Configuration files

- Switch A:

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
#
```

- Switch B:

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ip verify source ip-address
 ip source binding ip-address 192.168.0.2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
```

Related documentation

- IP source guard configuration in the security configuration guide for the device.
- IP source guard commands in the security command reference for the device.

SSH Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring the device as an SSH server 1

Introduction 1
Network configuration 1
Procedure 1
Verifying the configuration 2
Configuration files 4
Related documentation 5

Configuring the device as an SSH client 6

Introduction 6
Network configuration 6
Procedure 6
Verifying the configuration 6
Configuration files 7
Related documentation 7

Configuring the device as an SSH server

Introduction

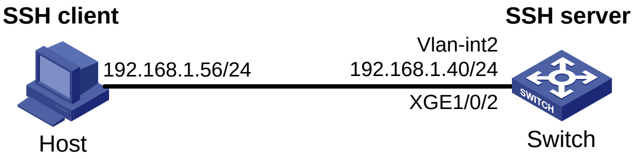
The following information uses an example to describe the basis procedure for configuring the device as an SSH server.

Network configuration

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

- The switch acts as the SSH server and uses password authentication to authenticate the SSH client locally.
- Set the username of the client to **client001** and password to **hello12345** for login. After the user logs in to the switch from the host, the user can use all commands to configure the switch.

Figure 1 Network diagram



Procedure

# Generate RSA key pairs.

```
<Switch> system-view
[Switch] 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.

```
[Switch] 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.

```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
```

```
.
Create the key pair successfully.
```

# Enable the SSH server.

```
[Switch] ssh server enable
```

# Create VLAN 2 and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] port ten-gigabitethernet 1/0/2
[Switch-vlan2] quit
```

# Assign an IP address to VLAN-interface 2. The SSH client uses this address as the destination for SSH connection.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

# Enable the login authentication mode to **scheme** for user lines VTY 0 through VTY 63.

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

# Create a local device management user named **client001**.

```
[Switch] local-user client001 class manage
New local user added.
```

# Set the password to **hello12345** in plain text for local user **client001**.

```
[Switch-luser-manage-client001] password simple hello12345
```

# Authorize local user **client001** to use the SSH service.

```
[Switch-luser-manage-client001] service-type ssh
```

# Assign the **network-admin** user role to local user **client001**.

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

Verifying the configuration

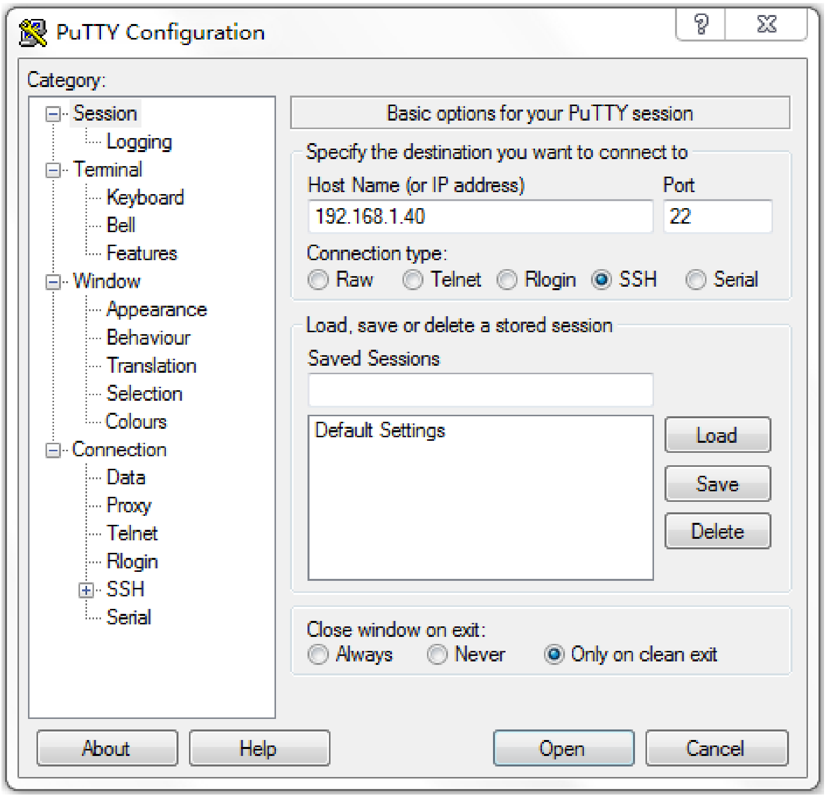
There are different types of SSH client software. This example uses an SSH client that runs PuTTY version 0.60 to verify the SSH login.

# Install PuTTY version 0.60 on the host.

# Launch PuTTY.exe. The PuTTY Configuration window opens. Click **Session**.

- In the **Host Name (or IP address)** field, enter IP address **192.168.1.40** of the SSH server.
- In the **Port** field, enter **22**.
- Select **SSH** as the connection type.

Figure 2 Configuring the SSH client



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.40

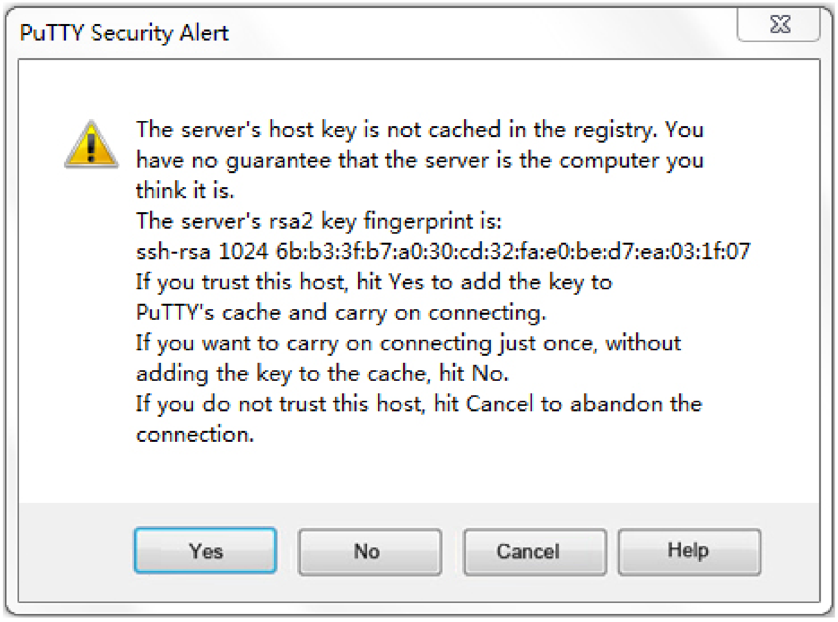
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

# Click **Open**. The **PuTTY Security Alert** dialog box opens.

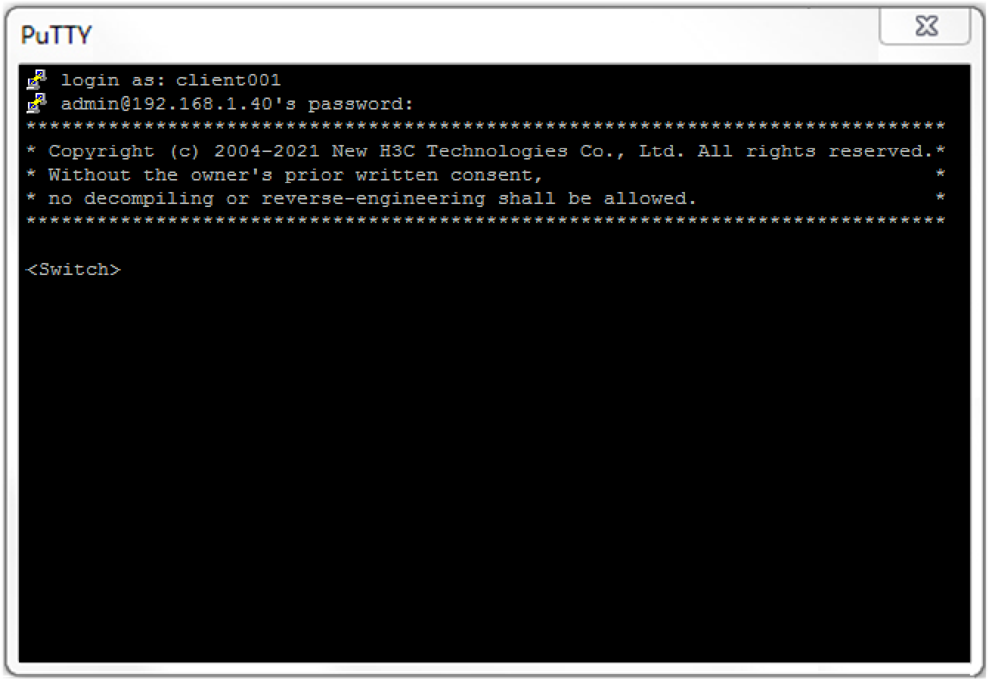
Figure 3 PuTTY Security Alert



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 6b:b3:3f:b7:a0:30:cd:32:fa:e0:be:d7:ea:03:1f:07
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

# Click **Yes**. Enter username **client001** and password **hello12345** (not shown on the interface) to log in to the SSH server.

Figure 4 Logging in to the SSH server



```
login as: client001
admin@192.168.1.40's 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.                    *
******************************************************************************

<Switch>
```

The output shows that you have successfully log in to the switch and can use all commands available on the switch.

Configuration files

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 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
#
```

Related documentation

- SSH configuration in the security configuration guide for the device.
- SSH commands in the security command reference for the device.

Configuring the device as an SSH client

Introduction

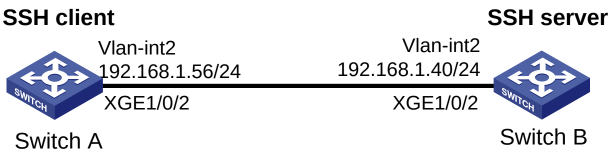
The following information uses an example to describe the basis procedure for configuring the device as an SSH client.

Network configuration

As shown in Figure 5, configure the switches to meet the following requirements:

- Switch A acts as the SSH client.
- Switch B acts as the SSH server and uses password authentication to authenticate the SSH client locally.
- Set the username of the client to **client001** and password to **hello12345** for login. After the user logs in to Switch B from Switch A, the user can use all commands to configure Switch B.

Figure 5 Network diagram



Procedure

1. Configure Switch A:

   # Create VLAN 2 and assign Ten-GigabitEthernet 1/0/2 to VLAN 2.

   ```
   <SwitchA> system-view
   [SwitchA] vlan 2
   [SwitchA-vlan2] port ten-gigabitethernet 1/0/2
   [SwitchA-vlan2] quit
   ```

   # Assign an IP address to VLAN-interface 2.

   ```
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   ```

2. Configure Switch B:

   # Configure Switch B as the SSH server. For more information, see "Configuring the device as an SSH server."

Verifying the configuration

Verify that you can successfully log in to Switch B as a network administrator:

# On Switch A, establish an SSH connection to the SSH server (Switch B) at 192.168.1.40.

# Enter username **client001** and enter **Y** to continue accessing the server without authenticating the server.

# Enter **N** to not save the server public key.

NOTE:

If you enter **Y** to save the server public key, when the server public key changes, execute the **`delete SSH client server public key`** command in the system view of Switch A to delete the saved public key, so that you can establish a connection to the server again.

# Enter password **hello12345** (not shown on the interface) to log in to the SSH server.

```
<SwitchA> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:Y
Do you want to save the server public key? [Y/N]:N
Enter 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.                    *
******************************************************************************

<SwitchB>
```

Configuration files

- Switch A

  ```
  #
  vlan 2
  #
  interface Vlan-interface2
  ip address 192.168.1.56 255.255.255.0
  #
  interface Ten-GigabitEthernet1/0/2
   port link-mode bridge
   port access vlan 2
  #
  ```

- Switch B

  See "Configuration files."

Related documentation

- SSH configuration in the security configuration guide for the device.
- SSH commands in the security command reference for the device.

Port Security Quick Start Configuration Guide

Contents

Configuring port security in autoLearn mode ·· 1

Introduction ·· 1

Network configuration ·· 1

Restrictions and guidelines ·· 1

Procedure ·· 1

Verifying the configuration ·· 2

Configuration files ·· 3

Related documentation ·· 4

Configuring port security in autoLearn mode

Introduction

The following information uses an example to describe the basic procedure for configuring a port in autoLearn mode for port security.

Network configuration

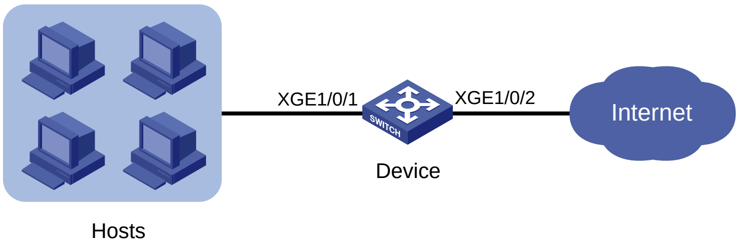
As shown in Figure 1, configure the user-attached port (Ten-GigabitEthernet 1/0/1 in this example) on the device to meet the following requirements:

- Allow up to 64 users to access the Internet through the port without authentication.
- Prevent additional users to access the Internet through the port after the number of online Internet users on the port reaches the limit.

To meet these requirements:

- Place the port in autoLearn mode. In this mode, the port learns and adds MAC addresses to the secure MAC address table until the specified limit is reached.
- Set port security's limit on the number of secure MAC addresses to 64.
- By default, secure MAC addresses do not age out. To prevent inactive or malicious users from using secure MAC table entries permanently, set a secure MAC aging timer.
- Set the intrusion protection action to disableport-temporarily. If a frame with an unknown MAC address arrives at the port when the secure MAC address table is full, shut down the port for 30 seconds.

Figure 1 Network diagram



Restrictions and guidelines

Set port security's limit on the number of secure MAC addresses on a port before you place that port in autoLearn mode. You cannot change the secure MAC address limit on a port in autoLearn mode.

Procedure

# 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 Ten-GigabitEthernet 1/0/1.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
```

# Place the port in autoLearn mode for port security.

```
[Device-Ten-GigabitEthernet1/0/1] port-security port-mode autolearn
```

# Set the intrusion protection action to disableport-temporarily and configure port security to shut down the port for 30 seconds after intrusion protection is triggered.

```
[Device-Ten-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30
```

Verifying the configuration

# Execute the **display port-security interface** command to verify that port security is correctly configured.

```
[Device] display port-security interface ten-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
   OUI value list         :

 Ten-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 output shows that the port allows a maximum of 64 secure MAC addresses, its port security mode is autoLearn, its intrusion protection action is DisablePortTemporarily, and it will shut down for 30 seconds after the intrusion protection action is triggered.

To view the number of secure MAC addresses learned on the port, examine the **Current secure MAC addresses** field.

# To view information about each secure MAC address, execute the **`display this`** command on the interface view for the port.

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] display this
#
interface Ten-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
#
```

# When the number of MAC addresses learned on the port reaches 64, execute the **`display port-security interface`** command to verify that the port security mode changes to secure mode. In secure mode, the port stops learning MAC addresses. (Details not shown.)

# After the port receives a frame with an unknown MAC address, execute the **`display interface`** command to verify that the port shuts down for intrusion protection and comes up 30 seconds later. (Details not shown.)

# Delete several secure MAC addresses. Verify that the port security mode changes to autoLearn and the port can learn MAC addresses again. (Details not shown.)

Configuration files

```
#
 port-security enable
 port-security timer disableport 30
 port-security timer autolearn aging 30
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port-security intrusion-mode disableport-temporarily
 port-security max-mac-count 64
 port-security port-mode autolearn
#
```

Related documentation

- Port security configuration in the security configuration guide for the device.
- Port security commands in the security command reference for the device.

VRRP Quick Start Configuration Guide

Contents

Configuring a single VRRP group ··· 1

Introduction ··· 1

Network configuration ··· 1

Restrictions and guidelines ··· 1

Procedure ··· 2

Verifying the configuration ··· 3

Configuration files ··· 4

Related documentation ··· 5

Configuring a single VRRP group

Introduction

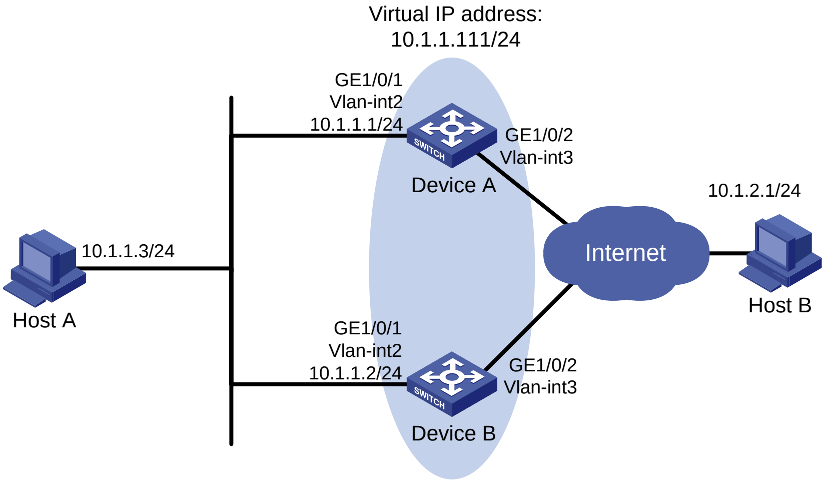
The following information uses an example to describe the basic procedure for configuring a single VRRP group.

Network configuration

As shown in Figure 1, Host A needs to access Host B on the Internet. Two devices are deployed at the network egress of Host A. Configure a VRRP group on Device A and Device B to act as the default gateway for Host A and implement the following requirements:

- Device A operates as the master to forward packets from Host A to Host B.
- When Device A fails, Device B takes over to forward packets for Host A.
- When Device A recovers, Device A acts as the gateway again.

Figure 1 Network diagram



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).

- You can specify the IPv4 VRRP version as VRRPv2 or VRRPv3 (default version). The version of VRRP on all routers in an IPv4 VRRP group must be the same.
- The virtual IP address of an IPv4 VRRP group and the downlink interface IP addresses of the VRRP group members must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.
- Make sure all members in a VRRP group have the same virtual IP address configured.
- Make sure the reduced priority is lower than the priority of any other devices in the VRRP group, so that another device can be elected as master.

Procedure

### Configure Device A

# Configure VLAN 2 and add 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 set its IP address to 10.1.1.1/24.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

# Create VRRP group 1 on VLAN-interface 2 and set its virtual IP address to 10.1.1.111.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

# Assign Device A 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, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

```
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[DeviceA-Vlan-interface2] quit
```

# Create track entry 1 associated with GigabitEthernet 1/0/2.

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

# Create track entry 1. When the track entry transits to Negative state, Device A decreases its priority by 50 in the VRRP group.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface2] quit
```

Configure Device B

# Configure VLAN 2.

```
<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 10.1.1.2 255.255.255.0
```

# Create VRRP group 1 on VLAN-interface 2 and set its virtual IP address to 10.1.1.111.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

# Set the priority of Device B to 100 in VRRP group 1.

```
[DeviceB-Vlan-interface2] vrrp vrid 1 priority 100
```

Verifying the configuration

# Ping Host B from Host A. (Details not shown.)

# 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   : 5000
     Auth Type      : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   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   : 0
     Become Master  : 401ms left
     Auth Type        : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Master IP        : 10.1.1.1
```

The output shows that Device A is operating as the master in VRRP group 1 to forward packets from Host A to Host B.

# When Device A fails, verify that Host A can still ping Host B. (Details not shown.)

# 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        : Master
     Config Pri     : 100                 Running Pri  : 100
     Preempt Mode   : Yes                 Delay Time   : 0
     Auth Type        : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Master IP        : 10.1.1.2
```

The output shows that when Device A fails, Device B takes over to forward packets from Host A to Host B.

# After Device A recovers, 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   : 5000
     Auth Type      : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50
```

The output shows that after Device A resumes normal operation, it becomes the master to forward packets from Host A to Host B.

Configuration files

- Device A:

```
#
```

```
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5000
 vrrp vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
 track 1 interface Ten-GigabitEthernet1/0/2
#
```

- Device B:

```
#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 100
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
```

Related documentation

- VRRP configuration in the high availability configuration guide for the device.
- VRRP commands in the high availability command reference for the device.

PoE Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring PoE ··· 1

Introduction ··· 1

Restrictions and guidelines ··· 1

Procedure ··· 1

Verifying the configuration ··· 2

Configuration files ··· 2

Related documentation ··· 2

Configuring PoE

Introduction

The following information uses an example to describe the basis procedure to configure PoE.

Restrictions and guidelines

The system reserves and supplies power to a PSE only after you enable PoE for that PSE.

You can enable PoE for a PSE if the PSE will not result in PoE power overload. If the PSE will result in PoE power overload, you can enable PoE for the PSE only when the PSE priority policy is enabled on the PSE.

You cannot execute the **apply poe-profile** or **apply poe-profile interface** command repeatedly to modify a PoE profile. To modify a PoE profile applied on a PI, first remove the PoE profile from the PI.

Procedure

Enabling PoE for a single PI

# Enter system view.

```
< Device> system-view
```

# Enable PoE on GigabitEthernet 1/0/1.

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] poe enable
[Device-GigabitEthernet1/0/1] quit
```

# Save the configuration.

```
[Device] save force
```

Enabling PoE for PIs in bulk

# Create a PoE profile named **abc**, and specify its index number as 1.

```
<Device> system-view
[Device] poe-profile abc 1
```

# Enable PoE.

```
[Device-poe-profile-abc-1] poe enable
[Device-poe-profile-abc-1] return
```

# Apply PoE profile **abc** with an index number of 1 to PIs.

```
<Device> system-view
[Device] apply poe-profile abc index 1 interface gigabitethernet 1/0/1 to gigabitethernet
1/0/6
```

# Save the configuration.

```
[Device] save force
```

Verifying the configuration

# Verify that the device is supplying power correctly to the PIs, and the PIs are operating correctly.

Configuration files

- Enabling PoE for a single PI.

  ```
  #
  interface GigabitEthernet 1/0/1
  poe enable
  #
  ```

- Enabling PoE for PIs in bulk.

  ```
  #
  poe-profile abc 1
   poe enable
   apply poe-profile index 1
  save force
  #
  ```

Related documentation

- PoE configuration in the network management and monitoring configuration guide for the device.
- PoE commands in the network management and monitoring command reference for the device.

Mirroring Quick Start Configuration Guide

Contents

Configuring local port mirroring 1

Introduction 1
Network configuration 1
Restrictions and guidelines 1
Procedure 1
Verifying the configuration 2
Configuration files 3
Related documentation 4

Configuring local port mirroring with multiple monitor ports through a remote probe VLAN 5

Introduction 5
Network configuration 5
Restrictions and guidelines 5
Procedure 5
Verifying the configuration 6
Configuration files 6
Related documentation 7

Configuring Layer 2 remote port mirroring in egress port mode 8

Introduction 8
Network configuration 8
Restrictions and guidelines 8
Procedures 9
Verifying the configuration 11
Configuration files 12
Related documentation 14

Configuring Layer 2 remote port mirroring in reflector port mode 15

Introduction 15
Network configuration 15
Restrictions and guidelines 15
Procedures 16
Verifying the configuration 18
Configuration files 18
Related documentation 19

Configuring Layer 3 remote port mirroring in encapsulation parameter mode 20

Introduction 20
Network configuration 20
Restrictions and guidelines 20
Procedures 20
Verifying the configuration 22
Configuration files 22
Related documentation 23

Configuring local flow mirroring 24

Introduction 24
Network configuration 24
Procedure 24
Verifying the configuration 25
Configuration files 25
Related documentation 26

Configuring local port mirroring

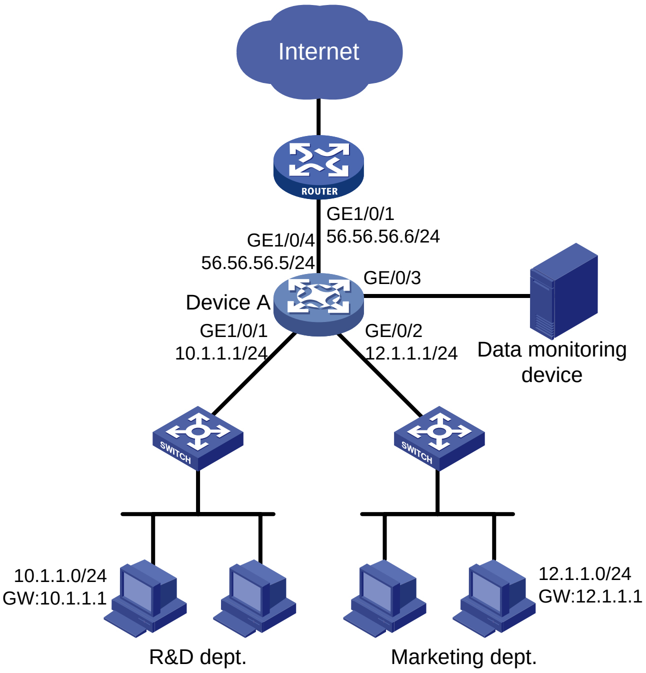
Introduction

The following information uses an example to describe the basic procedure for configuring local port mirroring.

Network configuration

The departments of a company use IP addresses on different subnets. The R&D department uses subnet 10.1.1.0/24, and the marketing department uses subnet 12.1.1.0/24. Configure local port mirroring, so that the data monitoring device can monitor the traffic from the R&D department and marketing department to Internet and the traffic between the two departments.

Figure 1 Network diagram



Restrictions and guidelines

- For a local mirroring group to take effect, you must configure the mirroring source ports and monitor port for the group. Make sure the monitor port is not the member port of any other mirroring group.
- A monitor port can receive both mirrored packets copied from source ports and normally forwarded packets from other ports. Use a monitor port only for port mirroring, so the data monitoring device receives and analyzes only the mirrored traffic.

Procedure

# Assign IP address 10.1.1.1/24 to GigabitEthernet 1/0/1, which connects to the device of the R&D department.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

# Assign IP address 12.1.1.1/24 to GigabitEthernet 1/0/2, which connects to the device of the marketing department.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 12.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

# Assign IP address 56.56.56.5/24 to GigabitEthernet 1/0/4.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-mode route
[DeviceA-GigabitEthernet1/0/4] ip address 56.56.56.5 24
[DeviceA-GigabitEthernet1/0/4] quit
```

# Create a local mirroring group.

```
[DeviceA] mirroring-group 1 local
```

# Configure the local mirroring group to mirror the incoming packets of interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2
inbound
```

# Configure interface GigabitEthernet 1/0/3 as the monitor port.

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

# Disable the spanning tree protocol on the monitor port, GigabitEthernet 1/0/3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

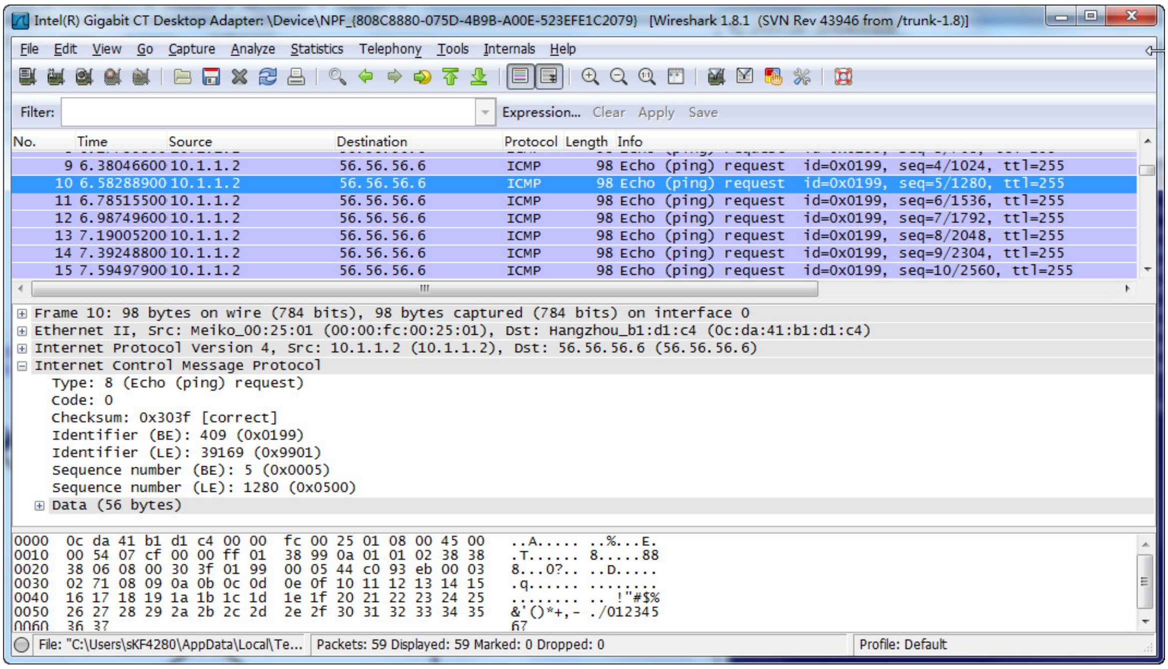
Verifying the configuration

# 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
```

# Ping 56.56.56.6 from a host at 10.1.1.2 in the R&D department. Capture the packets on the data monitoring device, as shown in Figure 2. In this example, use Wireshark to capture packets.

Figure 2 Packets captured by Wireshark



Intel(R) Gigabit CT Desktop Adapter: \Device\NPF_{808C8880-075D-4B9B-A00E-523EFE1C2079}   [Wireshark 1.8.1 (SVN Rev 43946 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time        Source     Destination  Protocol Length Info
    9 6.38046600 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=4/1024, ttl=255
   10 6.58288900 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=5/1280, ttl=255
   11 6.78515500 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=6/1536, ttl=255
   12 6.98749600 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=7/1792, ttl=255
   13 7.19005200 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=8/2048, ttl=255
   14 7.39248800 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=9/2304, ttl=255
   15 7.59497900 10.1.1.2   56.56.56.6   ICMP         98 Echo (ping) request  id=0x0199, seq=10/2560, ttl=255
```

```
⊞ Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
⊞ Ethernet II, Src: Meiko_00:25:01 (00:00:fc:00:25:01), Dst: Hangzhou_b1:d1:c4 (0c:da:41:b1:d1:c4)
⊞ Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 56.56.56.6 (56.56.56.6)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x303f [correct]
    Identifier (BE): 409 (0x0199)
    Identifier (LE): 39169 (0x9901)
    Sequence number (BE): 5 (0x0005)
    Sequence number (LE): 1280 (0x0500)
  ⊞ Data (56 bytes)
```

```
0000  0c da 41 b1 d1 c4 00 00  fc 00 25 01 08 00 45 00   ..A..... ..%...E.
0010  00 54 07 cf 00 00 ff 01  38 99 0a 01 01 02 38 38   .T...... 8.....88
0020  38 06 08 00 30 3f 01 99  00 05 44 c0 93 eb 00 03   8...0?.. ..D.....
0030  02 71 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   .q...... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

File: "C:\Users\sKF4280\AppData\Local\Te... Packets: 59 Displayed: 59 Marked: 0 Dropped: 0 Profile: Default

The captured packets show that the local port mirroring function takes effect. The data monitoring device can successfully monitor the specified traffic.

Configuration files

```
#
 mirroring-group 1 local
#
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 12.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 56.56.56.5 255.255.255.0
#
```

Related documentation

- Port mirroring configuration in the network management and monitoring configuration guide for the device.
- Port mirroring commands in the network management and monitoring command reference for the device.

Configuring local port mirroring with multiple monitor ports through a remote probe VLAN

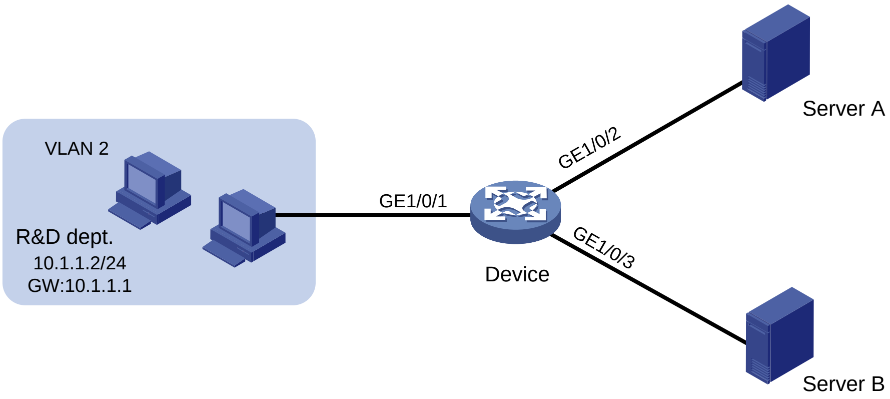
Introduction

The following information uses an example to describe the basic procedure for configuring local port mirroring with multiple monitor ports through the remote probe VLAN method.

Network configuration

The R&D department connects to Device through interface GigabitEthernet 1/0/1. Configure mirroring, so that the data monitoring devices Server A and Server B can monitor the incoming and outgoing packets of the R&D department.

Figure 3 Network diagram



Restrictions and guidelines

When a VLAN is configured as a remote probe VLAN, use the VLAN for port mirroring exclusively.

Only a static VLAN that already exists can be configured as a remote probe VLAN. A VLAN can be configured as the remote probe VLAN for only one mirroring group.

To delete a VLAN that is configured as a remote probe VLAN, first remove the remote probe VLAN configuration.

Procedure

# Create VLAN 2.

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

# Create VLAN-interface 2, and assign an IP address to it.

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 10.1.1.1 24
[Device-Vlan-interface2] quit
```

# Create VLAN 10, which is to be used as the remote probe VLAN.

```
[Device] vlan 10
[Device-vlan10] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk, and assign it to VLAN 2.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
[Device-GigabitEthernet1/0/1] port trunk permit vlan 2
[Device-GigabitEthernet1/0/1] quit
```

# Create remote source group 1.

```
<Device> system-view
[Device] mirroring-group 1 remote-source
```

# Configure GigabitEthernet 1/0/1, which connects to the R&D department, as the source port of remote source group 1.

```
[Device] mirroring-group 1 mirroring-port gigabitethernet1/0/1 both
```

# Configure an unused port (GigabitEthernet 1/0/4 in this example) as the reflector port of mirroring group 1.

```
[Device] mirroring-group 1 reflector-port gigabitethernet1/0/4
This operation may delete all settings made on the interface. Continue? [Y/N]:y
```

# Assign the interfaces connecting to data monitoring devices to VLAN 10.

```
[Device] vlan 10
[Device-vlan10] port gigabitethernet1/0/2 to gigabitethernet1/0/3
[Device-vlan10] quit
```

# Configure VLAN 10 as the remote probe VLAN of mirroring group 1.

```
[Device] mirroring-group 1 remote-probe vlan 10
```

Verifying the configuration

# Display information about mirroring group 1 on Device.

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Reflector port: GigabitEthernet1/0/4
    Remote probe VLAN: 10
```

Configuration files

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 10
```

```
#
vlan 2
#
vlan 10
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2
 mirroring-group 1 mirroring-port inbound
#
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 10
 mirroring-group 1 reflector-port
#
```

Related documentation

- Port mirroring configuration in the network management and monitoring configuration guide for the device.
- Port mirroring commands in the network management and monitoring command reference for the device.

Configuring Layer 2 remote port mirroring in egress port mode

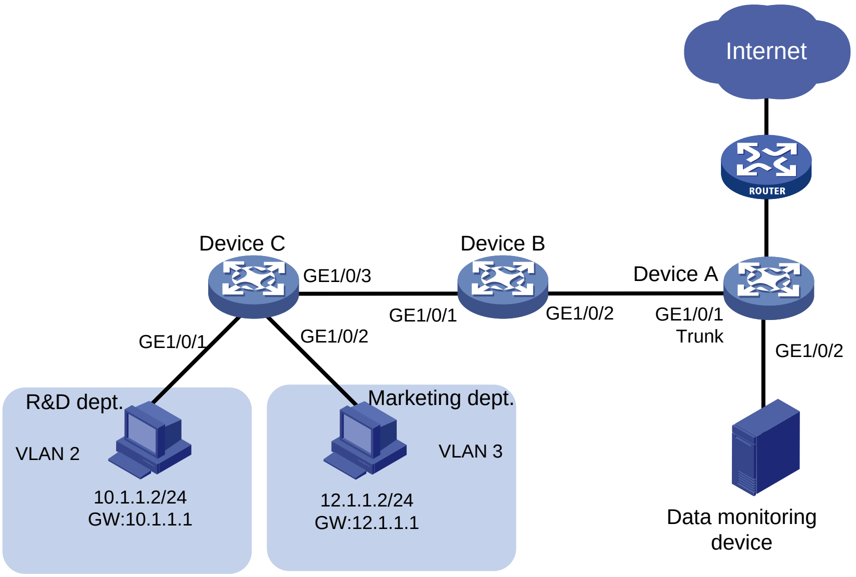
Introduction

The following information uses an example to describe the basic procedure for configuring Layer 2 remote port mirroring in egress port mode.

Network configuration

The departments of a company access the core device Device A through a Layer 2 network and these departments use IP addresses on different subnets. The R&D department uses subnet 10.1.1.0/24, and the marketing department uses subnet 12.1.1.0/24. Configure Layer 2 remote port mirroring in egress port mode, so that the data monitoring device can monitor the traffic from the R&D department.

Figure 4 Network diagram



Restrictions and guidelines

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.

As a best practice to ensure mirrored packet forwarding, configure mirroring on devices in the order of destination device, intermediate devices, and source device.

When configuring remote port mirroring on the destination device and source device, follow these restrictions and guidelines:

- When configuring a remote probe VLAN, follow these restrictions and guidelines:
  - Make sure the VLAN is an existing static VLAN.
  - Use the VLAN for remote port mirroring only.

    - The VLAN can be used by only one remote source group.
- Make sure the remote mirroring groups on the source device and destination device use the same remote probe VLAN.

When configuring remote port mirroring on the destination device, follow these restrictions and guidelines:

- Make sure the monitor port is not the member port of any other mirroring group.
- Use the monitor port for port mirroring only.

When configuring remote port mirroring on the source device, follow these restrictions and guidelines:

- For mirroring to operate correctly, do not assign source ports to the remote probe VLAN.
- For mirroring to operate properly, do not configure any of the following features on the egress port:
    - Spanning tree protocols.
    - 802.1X.
    - IGMP snooping.
    - Static ARP.
    - MAC address learning.
- Make sure the egress port is not the member port of any other mirroring group.
- A mirroring group supports only one egress port.
- When source ports are Layer 3 interfaces, you can implement Layer 2 remote mirroring only in egress port mode.

Procedures

Configuring Device A (destination device)

# Create VLANs 2 and 3.

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
```

# Create VLAN-interface 2, and assign an IP address to it, which is to be used as the gateway for the VLAN. Configure VLAN-interface 3 in the same way.

```
[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
```

# Set the link type of GigabitEthernet 1/0/1 to trunk, and assign it 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
```

# Create remote destination group 1.

```
[DeviceA] mirroring-group 1 remote-destination
```

# Configure VLAN 5 as the remote probe VLAN for the remote destination group. Configure GigabitEthernet 1/0/2, which connects to the data monitoring device, as the monitor port of remote destination group 1.

```
[DeviceA] mirroring-group 1 remote-probe vlan 5
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

# Add the monitor port to the remote probe VLAN. When the mirrored packets are sent to the data monitoring device, they do not carry the tag of the remote probe VLAN. Therefore, set the link type of the interface to access.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 5
```

# Disable the spanning tree protocol on the monitor port, GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B (intermediate device)

# Create VLANs 2 and 3.

```
<DeviceB> system-view
[DeviceB] vlan 2 to 3
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceB] vlan 5
[DeviceB-vlan5] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk, and assign it 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
```

# Set the link type of GigabitEthernet 1/0/2 to trunk, and assign it 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 (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 remote source group 1.

```
[DeviceC] mirroring-group 1 remote-source
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceC] vlan 5
```

```
[DeviceC-vlan5] quit
```

# Configure VLAN 5 as the remote probe VLAN, configure GigabitEthernet 1/0/1 as the source port, and configure GigabitEthernet 1/0/3 as the egress port for remote source group 1.

```
[DeviceC] mirroring-group 1 remote-probe vlan 5
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
[DeviceC] mirroring-group 1 monitor-egress gigabitethernet 1/0/3
```

# Set the link type of GigabitEthernet 1/0/3 to trunk, and assign it 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 protocol on the egress port, GigabitEthernet 1/0/3.

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] quit
```

Verifying the configuration

# Display information about mirroring group 1 on Device C.

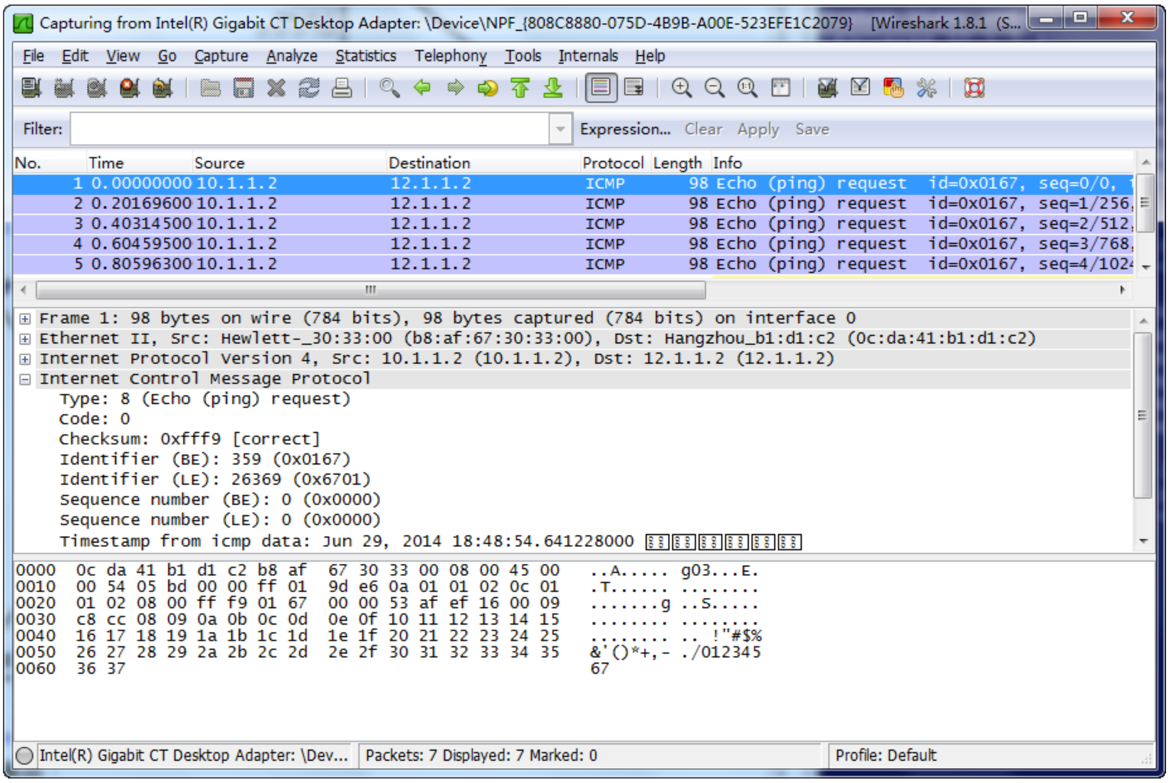
```
[DeviceC] display mirroring-group 1
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor egress port: GigabitEthernet1/0/3
        Remote probe VLAN: 5
```

# Display information about mirroring group 1 on Device A.

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

# Ping a host at 12.1.1.2 in the marketing department from a host at 10.1.1.2 in the R&D department. Capture the packets on the data monitoring device, as shown in Figure 5. In this example, use Wireshark to capture packets.

Figure 5 Packets captured by Wireshark


Capturing from Intel(R) Gigabit CT Desktop Adapter: \Device\NPF_{808C8880-075D-4B9B-A00E-523EFE1C2079} [Wireshark 1.8.1 (S...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.     Time        Source       Destination   Protocol Length Info
      1 0.00000000 10.1.1.2     12.1.1.2      ICMP       98 Echo (ping) request  id=0x0167, seq=0/0,
      2 0.20169600 10.1.1.2     12.1.1.2      ICMP       98 Echo (ping) request  id=0x0167, seq=1/256,
      3 0.40314500 10.1.1.2     12.1.1.2      ICMP       98 Echo (ping) request  id=0x0167, seq=2/512,
      4 0.60459500 10.1.1.2     12.1.1.2      ICMP       98 Echo (ping) request  id=0x0167, seq=3/768,
      5 0.80596300 10.1.1.2     12.1.1.2      ICMP       98 Echo (ping) request  id=0x0167, seq=4/102
```

```
⊞ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
⊞ Ethernet II, Src: Hewlett-_30:33:00 (b8:af:67:30:33:00), Dst: Hangzhou_b1:d1:c2 (0c:da:41:b1:d1:c2)
⊞ Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 12.1.1.2 (12.1.1.2)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xfff9 [correct]
    Identifier (BE): 359 (0x0167)
    Identifier (LE): 26369 (0x6701)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    Timestamp from icmp data: Jun 29, 2014 18:48:54.641228000 □□□□□□
```

```
0000  0c da 41 b1 d1 c2 b8 af  67 30 33 00 08 00 45 00   ..A..... g03...E.
0010  00 54 05 bd 00 00 ff 01  9d e6 0a 01 01 02 0c 01   .T...... ........
0020  01 02 08 00 ff f9 01 67  00 00 53 af ef 16 00 09   .......g ..S.....
0030  c8 cc 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Intel(R) Gigabit CT Desktop Adapter: \Dev...
Packets: 7 Displayed: 7 Marked: 0
Profile: Default

The captured packets show that the Layer 2 remote port mirroring function takes effect. The data monitoring device can monitor the packets sent by the R&D department.

Configuration files

- 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 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
#
```

Related documentation

- Port mirroring configuration in the network management and monitoring configuration guide for the device.
- Port mirroring commands in the network management and monitoring command reference for the device.

Configuring Layer 2 remote port mirroring in reflector port mode

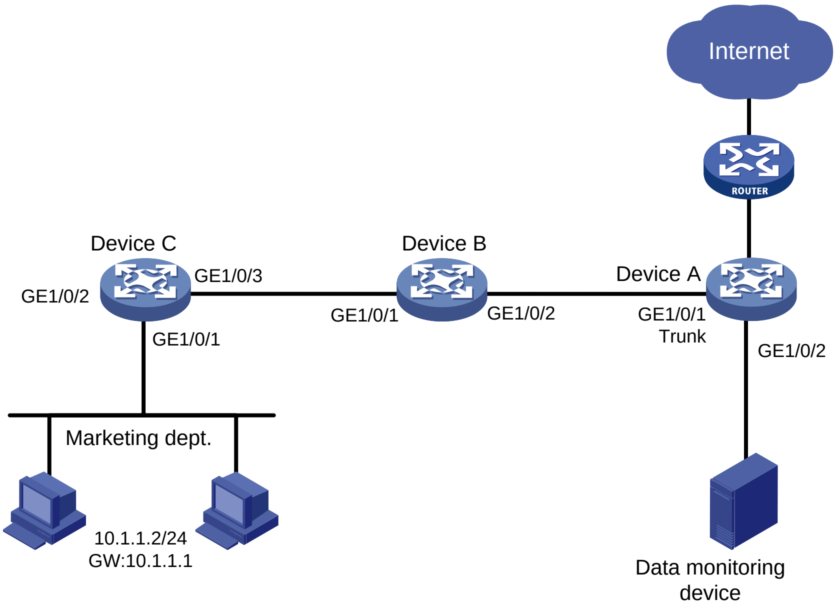
Introduction

The following information uses an example to describe the basic procedure for configuring Layer 2 remote port mirroring in reflector port mode.

Network configuration

The marketing department of a company connects to the core device Device A through a Layer 2 network, and uses the subnet 10.1.1.0/24. Configure Layer 2 remote port mirroring in reflector port mode, so that the data monitoring device can monitor the traffic from the marketing department.

Figure 6 Network diagram



Restrictions and guidelines

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.

As a best practice to ensure mirrored packet forwarding, configure mirroring on devices in the order of destination device, intermediate devices, and source device.

When configuring remote port mirroring on the destination device and source device, follow these restrictions and guidelines:

- When configuring a remote probe VLAN, follow these restrictions and guidelines:
  - Make sure the VLAN is an existing static VLAN.
  - Use the VLAN for remote port mirroring only.
  - The VLAN can be used by only one remote source group.

- Make sure the remote mirroring groups on the source device and destination device use the same remote probe VLAN.

When configuring remote port mirroring on the destination device, follow these restrictions and guidelines:

- Make sure the monitor port is not the member port of any other mirroring group.
- Use the monitor port for port mirroring only.

When configuring remote port mirroring on the source device, follow these restrictions and guidelines:

- For mirroring to operate correctly, do not assign source ports to the remote probe VLAN.
- The port to be configured as a reflector port must be a port not in use. Do not connect a network cable to a reflector port.
- When a port is configured as a reflector port, the port restores to the factory default settings. You cannot configure other features on a reflector port.
- If an IRF port is bound to only one physical interface, do not configure the physical interface as a reflector port. If you do that, the IRF might split.

Procedures

Configuring Device A (destination device)

# Create VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
```

# Create VLAN-interface 2, and assign an IP address to it, which is to be used as the gateway for the VLAN.

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk, and assign it to VLANs 2 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 5
[DeviceA-GigabitEthernet1/0/1] quit
```

# Create remote destination group 1.

```
[DeviceA] mirroring-group 1 remote-destination
```

# Configure VLAN 5 as the remote probe VLAN for the remote destination group. Configure GigabitEthernet 1/0/2, which connects to the data monitoring device, as the monitor port of remote destination group 1.

```
[DeviceA] mirroring-group 1 remote-probe vlan 5
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

# Add the monitor port to the remote probe VLAN. When the mirrored packets are sent to the data monitoring device, they do not carry the tag of the remote probe VLAN. Therefore, set the link type of the interface to access.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 5
```

# Disable the spanning tree protocol on the monitor port, GigabitEthernet 1/0/2.

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

Configuring Device B (intermediate device)

# Create VLAN 2.

```
<DeviceB> system-view
[DeviceB] vlan 2
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceB] vlan 5
[DeviceB-vlan5] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk, and assign it to VLANs 2 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 5
[DeviceB-GigabitEthernet1/0/1] quit
```

# Set the link type of GigabitEthernet 1/0/2 to trunk, and assign it to VLANs 2 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 5
[DeviceB-GigabitEthernet1/0/2] quit
```

Configuring Device C (source device)

# Create VLAN 2.

```
<DeviceC> system-view
[DeviceC] vlan 2
```

# 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
```

# Create remote source group 1.

```
[DeviceC] mirroring-group 1 remote-source
```

# Create VLAN 5, which is to be used as the remote probe VLAN.

```
[DeviceC] vlan 5
[DeviceC-vlan5] quit
```

# Configure VLAN 5 as the remote probe VLAN, configure GigabitEthernet 1/0/1 as the source port, and configure GigabitEthernet 1/0/2 as the reflector port for remote source group 1.

```
[DeviceC] mirroring-group 1 remote-probe vlan 5
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
[DeviceC] mirroring-group 1 reflector-port gigabitethernet 1/0/2
```

# Set the link type of GigabitEthernet 1/0/3 to trunk, and assign it to VLANs 2 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
[DeviceC-GigabitEthernet1/0/3] quit
```

Verifying the configuration

# Display configuration information of all mirroring groups on Device A.

```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

# Display configuration information of all mirroring groups on Device C.

```
[DeviceC] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  inbound
    Reflector port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

Configuration files

- Device A:

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 5
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
 undo stp enable
 mirroring-group 1 monitor-port
#
```

- Device B:

```
#
vlan 2
```

```
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
```

- Device C:

```
#
 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
 mirroring-group 1 reflector-port
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 5
#
```

Related documentation

- Port mirroring configuration in the network management and monitoring configuration guide for the device.
- Port mirroring commands in the network management and monitoring command reference for the device.

Configuring Layer 3 remote port mirroring in encapsulation parameter mode

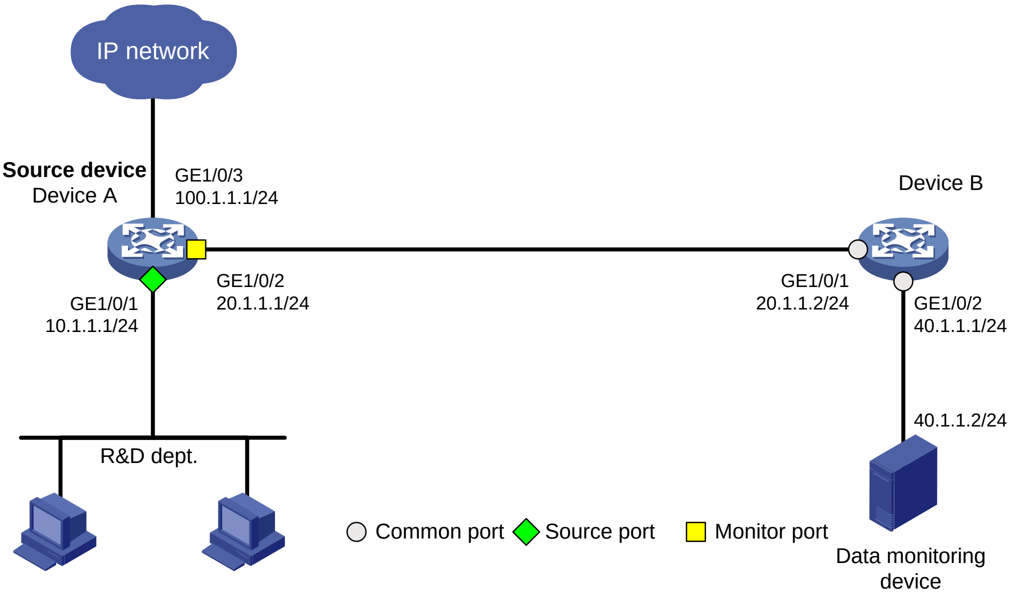
Introduction

The following information uses an example to describe the basic procedure for configuring Layer 3 remote port mirroring in encapsulation parameter mode.

Network configuration

The R&D department uses the subnet 10.1.1.0/24. Configure Layer 3 remote port mirroring, so that the data monitoring device can monitor the traffic from the R&D department to Internet.

Figure 7 Network diagram



Restrictions and guidelines

If intermediate devices exist between the source device and the destination device, configure a unicast routing protocol on the intermediate devices to ensure that the source device and the destination device can reach each other at Layer 3.

Procedures

Configuring Device A

# Assign IP address 10.1.1.1 to interface GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

# Assign IP address 20.1.1.1 to interface GigabitEthernet 1/0/2.

```
[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 address 100.1.1.1 to interface GigabitEthernet 1/0/3.

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-mode route
[DeviceA-GigabitEthernet1/0/3] ip address 100.1.1.1 24
[DeviceA-GigabitEthernet1/0/3] quit
```

# Configure OSPF.

```
<DeviceB> system-view
[DeviceB] ospf 1
[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] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-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

# Assign IP address 20.1.1.2 to interface GigabitEthernet 1/0/1.

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 20.1.1.2 24
[DeviceA-GigabitEthernet1/0/1] quit
```

# Assign IP address 40.1.1.1 to interface GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 40.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

# 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
#
```

- 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
#
```

Related documentation

- Port mirroring configuration in the network management and monitoring configuration guide for the device.
- Port mirroring commands in the network management and monitoring command reference for the device.

Configuring local flow mirroring

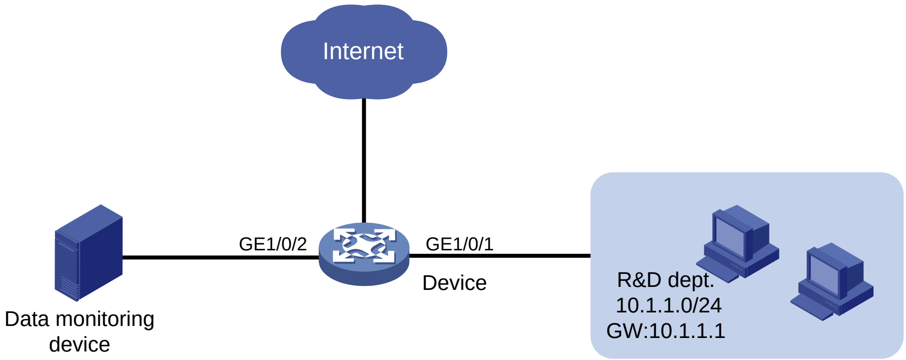
Introduction

The following information uses an example to describe the basic procedure for configuring local flow mirroring.

Network configuration

The R&D department of a company uses the 10.1.1.1/24 subnet. Configure local flow mirroring to enable the data monitoring device to monitor the WWW traffic from hosts in the R&D department to Internet.

Figure 8 Network diagram



Procedure

# Assign IP address 10.1.1.1/24 to GigabitEthernet 1/0/1, which connects to the device of the R&D department.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-mode route
[Device-GigabitEthernet1/0/1] ip address 10.1.1.0 24
[Device-GigabitEthernet1/0/1] quit
```

# Create ACL 3000, and configure a rule to match the traffic from the R&D department to Internet.

```
[Device] acl number 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq www source 10.1.1.0 0.0.0.255
[Device-acl-adv-3000] quit
```

# Create traffic class **classifier_research**, and use ACL 3000 as a match criterion.

```
[Device] traffic classifier classifier_research
[Device-classifier-classifier_research] if-match acl 3000
[Device-classifier-classifier_research] quit
```

# Create traffic behavior **behavior_research**, and configure an action of mirroring traffic to interface GigabitEthernet 1/0/2.

```
[Device] traffic behavior behavior_research
[Device-behavior-behavior_research] mirror-to interface gigabitethernet 1/0/2
```

```
[Device-behavior-behavior_research] quit
```

# Create QoS policy **policy_research**. Associate traffic class **classifier_research** with traffic behavior **behavior_research**.

```
[Device] qos policy policy_research
[Device-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[Device-qospolicy-policy_research] quit
```

# Apply QoS policy **policy_research** to the inbound direction of interface GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# Display the flow mirroring configuration information on Device.

```
[Device] 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
```

Configuration files

```
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
#
traffic classifier classifier_research operator and
 if-match acl 3000
#
traffic behavior behavior_research
 mirror-to interface GigabitEthernet1/0/2
#
qos policy policy_research
 classifier classifier_research behavior behavior_research
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.0 0.0.0.255
 qos apply policy policy_research inbound
#
```

Related documentation

- Flow mirroring configuration in the network management and monitoring configuration guide for the device.
- Flow mirroring commands in the network management and monitoring command reference for the device.

Information Center Quick Start Configuration Guide

The information in this document is subject to change without notice.

Contents

Configuring the device to output logs to a log host server ······························ 1

Introduction ······ 1
Network configuration ······ 1
Prerequisites ······ 1
Procedure······ 1
Verifying the configuration······ 2
Configuration files ······ 4
Related documentation ······ 4

Configuring the device to save logs to a specific folder in the flash drive ······· 5

Introduction ······ 5
Network configuration ······ 5
Restrictions and guidelines ······ 5
Procedure······ 5
Verifying the configuration······ 6
Configuration files ······ 6
Related documentation ······ 7

Configuring the device to output logs to a log host server

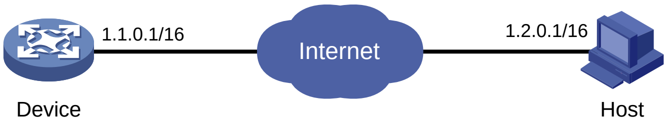
Introduction

The following information uses an example to describe the basic procedure for configuring the device to output logs to a log host server.

Network configuration

As shown in Figure 1, configure the device to output logs with severity levels from 0 through 7 to the log host server.

Figure 1 Network diagram



Prerequisites

- Configure IP addresses and routes. Make sure the device and the log host can reach each other. (Details not shown.)
- Install 3CDaemon on the host as a log host server.

Procedure

1. Configure the device:

   # Enable the information center.

   ```
   <Device> system-view
   [Device] info-center enable
   ```

   # Specify log host 1.2.0.1/16 with **local7** as the logging facility.

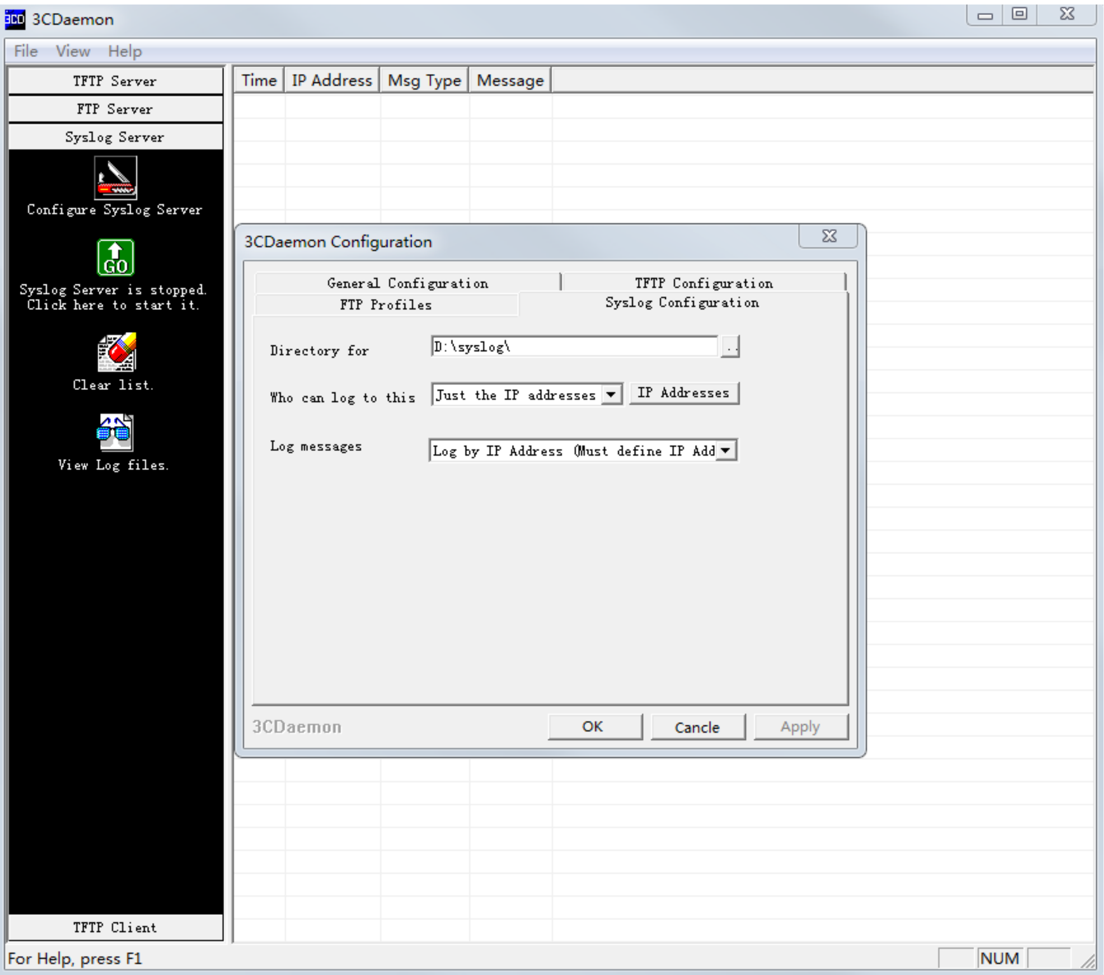
   ```
   [Device] info-center loghost 1.2.0.1 facility local7
   ```

2. Configure the log host:

   The log host server configuration procedure varies by the vendor. The following example uses 3CDaemon as the log host server to receive the logs sent by the switch.

   # Open 3CDaemon and complete corresponding configurations.

Figure 2 Configuring 3CDaemon as the log host server



Directory for: D:\syslog\

Who can log to this: Just the IP addresses

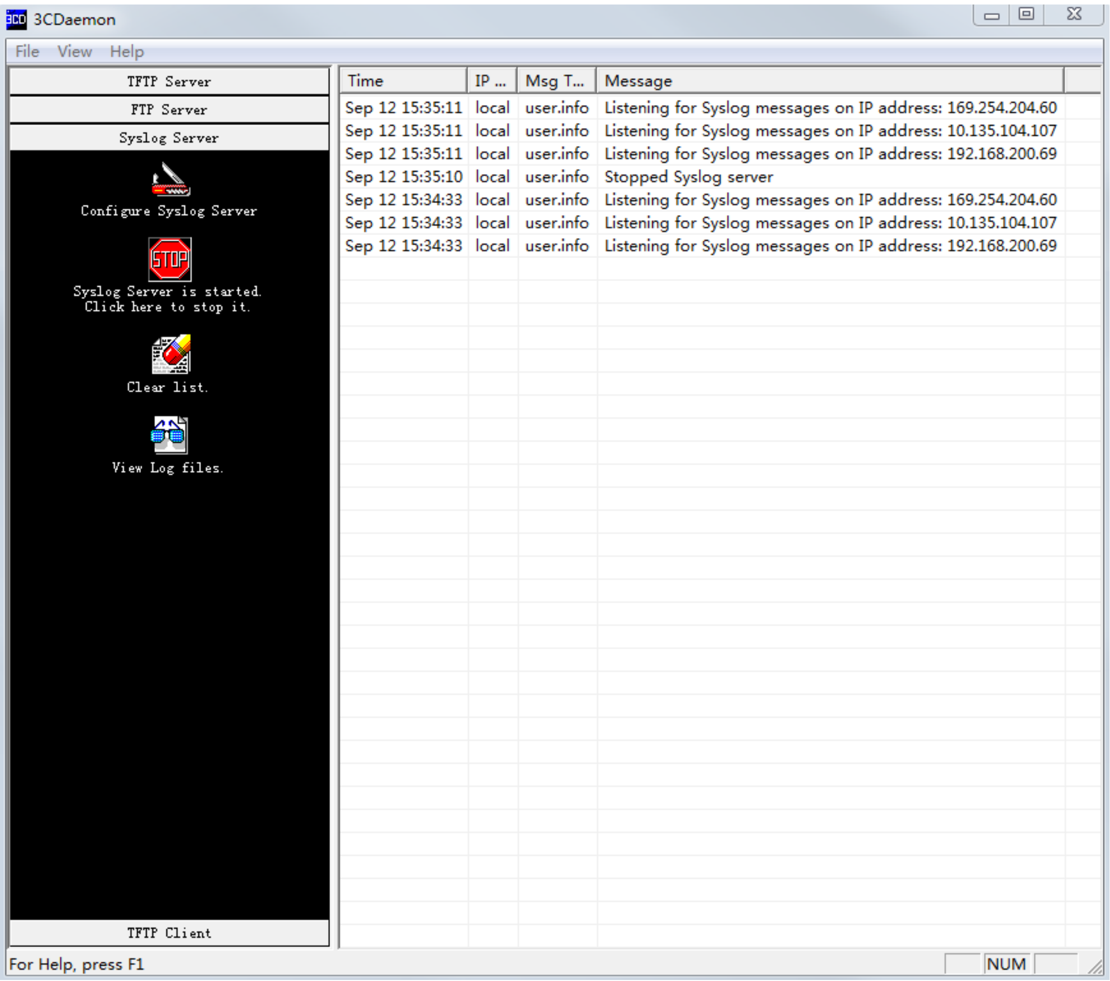
Log messages: Log by IP Address (Must define IP Add

# Launch the log host server.

Verifying the configuration

# Verify that you can view logs sent by the switch on the log host server.

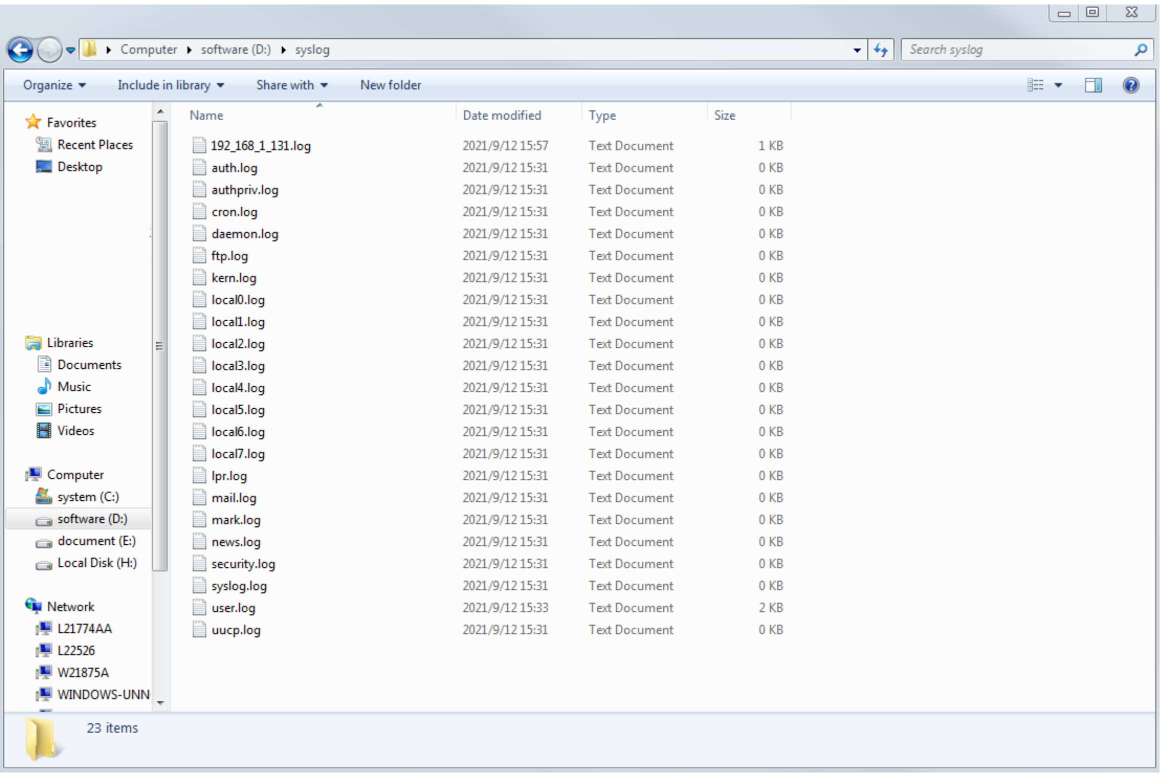
Figure 3 Viewing logs on 3CDaemon



```
Time             IP ...  Msg T...   Message
Sep 12 15:35:11  local   user.info  Listening for Syslog messages on IP address: 169.254.204.60
Sep 12 15:35:11  local   user.info  Listening for Syslog messages on IP address: 10.135.104.107
Sep 12 15:35:11  local   user.info  Listening for Syslog messages on IP address: 192.168.200.69
Sep 12 15:35:10  local   user.info  Stopped Syslog server
Sep 12 15:34:33  local   user.info  Listening for Syslog messages on IP address: 169.254.204.60
Sep 12 15:34:33  local   user.info  Listening for Syslog messages on IP address: 10.135.104.107
Sep 12 15:34:33  local   user.info  Listening for Syslog messages on IP address: 192.168.200.69
```

# Open the directory where the log files are saved to view logs.

Figure 4 Viewing log file directory



Name	Date modified	Type	Size
192_168_1_131.log	2021/9/12 15:57	Text Document	1 KB
auth.log	2021/9/12 15:31	Text Document	0 KB
authpriv.log	2021/9/12 15:31	Text Document	0 KB
cron.log	2021/9/12 15:31	Text Document	0 KB
daemon.log	2021/9/12 15:31	Text Document	0 KB
ftp.log	2021/9/12 15:31	Text Document	0 KB
kern.log	2021/9/12 15:31	Text Document	0 KB
local0.log	2021/9/12 15:31	Text Document	0 KB
local1.log	2021/9/12 15:31	Text Document	0 KB
local2.log	2021/9/12 15:31	Text Document	0 KB
local3.log	2021/9/12 15:31	Text Document	0 KB
local4.log	2021/9/12 15:31	Text Document	0 KB
local5.log	2021/9/12 15:31	Text Document	0 KB
local6.log	2021/9/12 15:31	Text Document	0 KB
local7.log	2021/9/12 15:31	Text Document	0 KB
lpr.log	2021/9/12 15:31	Text Document	0 KB
mail.log	2021/9/12 15:31	Text Document	0 KB
mark.log	2021/9/12 15:31	Text Document	0 KB
news.log	2021/9/12 15:31	Text Document	0 KB
security.log	2021/9/12 15:31	Text Document	0 KB
syslog.log	2021/9/12 15:31	Text Document	0 KB
user.log	2021/9/12 15:33	Text Document	2 KB
uucp.log	2021/9/12 15:31	Text Document	0 KB

Configuration files

```
#
info-center enable
 info-center loghost 1.2.0.1 facility local7
#
```

Related documentation

- Information center configuration in the network management and monitoring configuration guide for the device.
- Information center commands in the network management and monitoring command reference for the device.

Configuring the device to save logs to a specific folder in the flash drive

Introduction

The following information uses an example to describe the basic procedure for configuring the device to save logs to a specific folder in the flash drive.

Network configuration

- Configure the device to output logs with severity levels from 0 through 7 to a log file in the flash drive. Set the maximum log file size to 1 MB.
- Log user logins and commands executed by the user after login.
- Save the logs to the log buffer before saving them to the log file. Set the maximum number of logs that can be buffered to 500. Set the log file saving interval to 60000 seconds.
- Set the timestamp format to **boot** for output logs.

Restrictions and guidelines

The log file feature saves logs from the log file buffer to the log file at the specified saving interval. You can also manually trigger an immediate saving of buffered logs to the log file. After saving logs to the log file, the system clears the log file buffer.

Procedure

# Enter system view.

```
<Device> system-view
```

# Configure an output rule for sending logs with severity levels from 0 through 7 to the log buffer.

```
[Device] info-center source default logbuffer level debugging
```

# Enable log output to the log buffer.

```
[Device] info-center logbuffer
```

# Set the maximum number of logs that can be buffered to 500.

```
[Device] info-center logbuffer size 500
```

# Configure output of logs with severity levels from 0 through 7 to the log file.

```
[Device] info-center source default logfile level debugging
```

# Enable the log file feature.

```
[Device] info-center logfile enable
```

# Set the maximum log file size to 1 MB.

```
[Device] info-center logfile size-quota 1
```

# Configure the device to save logs to the **flash:/test** directory.

```
[Device] info-center logfile directory flash:/test
```

# Set the log file saving interval to 60000 seconds.

```
[Device] info-center logfile frequency 60000
```

# Set the timestamp format to **boot** for output logs.

```
[Device] info-center timestamp boot
```

Verifying the configuration

# View the summary of log file configurations.

```
[Device] display logfile summary
  Log file: Enabled
  Log file size quota: 1 MB
  Log file directory: flash:/test
  Writing frequency: 16 hour 40 min 0 sec
```

The output shows that the log file feature is enabled, the maximum log file size is 1 MB, the log file directory is **flash:/test**, and the log file saving interval is 60000 seconds.

# View information about the log buffer and the buffered logs.

```
[Device] display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 500
Dropped messages: 0
Overwritten messages: 402788
Current messages: 500
---- More ----
```

The output shows that log output to the log buffer is enabled, the maximum log file buffer size is 1 MB, and the maximum number of logs that can be buffered is 500.

# View the logs sent to the **flash:/test** directory.

```
[Device] more test/logfile.log
%@3049495%0.2409505789 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049496%0.2409506971 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 10.1.1.2 was n
ot the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049497%0.2409510823 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 10.1.1.2 was n
ot the IP of the receiving interface M-GigabitEthernet0/0/0. This message repeat
ed 2 times in last 3 seconds.
%@3049498%0.2409510789 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049499%0.2409520259 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0. This message re
peated 1 times in last 10 seconds.
---- More ----
```

Configuration files

```
#
info-center timestamp boot
 info-center logfile frequency 6000
 info-center logfile size-quota 1
 info-center source default monitor deny
 info-center source default logbuffer level debugging
 info-center source default logfile level debugging
#
```

Related documentation

- Information center configuration in the network management and monitoring configuration guide for the device.
- Information center commands in the network management and monitoring command reference for the device.

SNMP Quick Start Configuration Guide

Contents

Configuring SNMPv1/v2c ········ 1

Introduction ········ 1
Network configuration ········ 1
Restrictions and guidelines ········ 1
Procedure ········ 1
Verifying the configuration ········ 3
Configuration files ········ 3
Related documentation ········ 3

Configuring SNMPv3 ········ 4

Introduction ········ 4
Network configuration ········ 4
Restrictions and guidelines ········ 4
Procedure ········ 5
Configuring the device ········ 5
Configuring the IMC server ········ 6
Verifying the configuration ········ 7
Configuration files ········ 8
Related documentation ········ 8

Configuring SNMPv1/v2c

Introduction

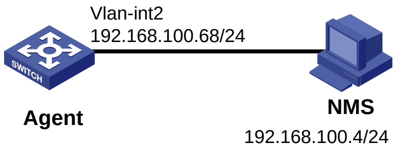
The following information uses an example to describe the basic SNMPv1/v2c configuration procedure.

Network configuration

As shown in Figure 1, configure the device (agent) and IMC server (NMS) to meet the following requirements:

- Enable the IMC server to monitor and manage the device through SNMPv1/SNMPv2c as an NMS.
- Enable the device to automatically send notifications to report events to the NMS as an agent.

Figure 1 Network diagram



Restrictions and guidelines

- The configuration procedure is the same for SNMPv1 and SNMPv2c. SNMPv2c is configured in this example.
- Configure the same SNMP version and community string on the device and the NMS so that the NMS can monitor and manage the device.
- The NMS configuration method varies by vendor. For information about configuring the NMS, see the manual for the NMS. This example uses the IMC PLAT 7.0 (E0202) NMS.

Procedure

Configuring the device

# Assign an IP address to VLAN-interface 2.

```
<Agent> system-view
[Agent] interface Vlan-interface 2
[Agent-Vlan-interface 2] ip address 192.168.100.68 24
[Agent-Vlan-interface 2] quit
```

# Specify SNMPv2c, and create read-only community string **readtest** and read-write community string **writetest**.

```
[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 device.

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

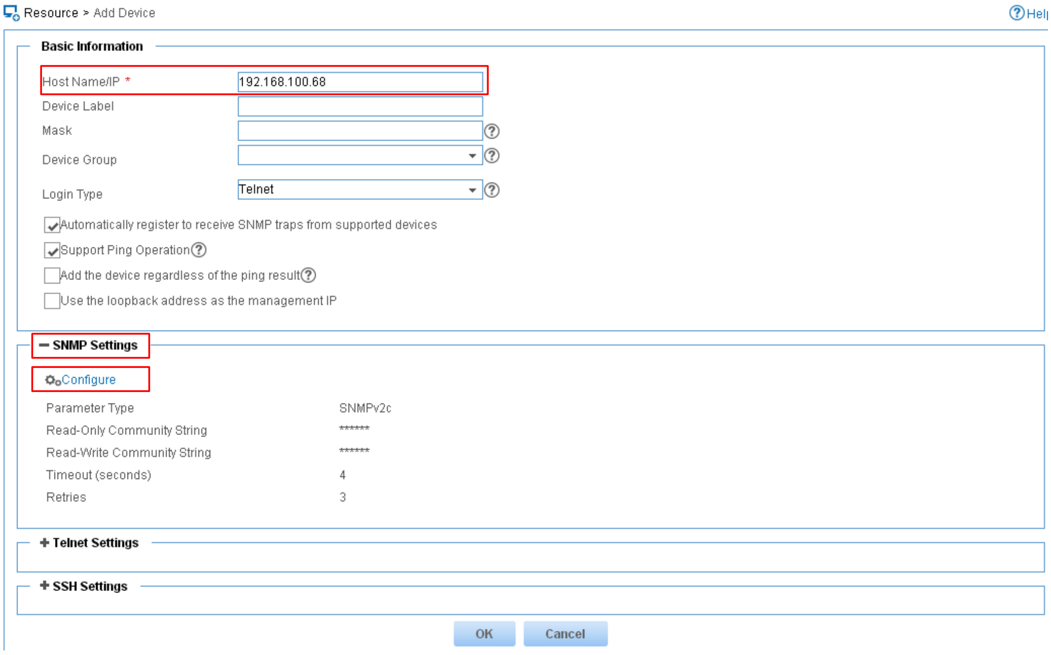
# Enable the device to send SNMP notifications to the NMS (IMC server) at 192.168.100.4 by using community string **readtest**.

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
readtest v2c
```

Configuring the IMC server

1. Log in to the IMC server.
2. Add the device to the IMC server:
   a. Click the **Resource** tab.
   b. From the navigation tree, select **Add Device**.
   c. Configure the following parameters on the page that opens:
      – Enter the host name or IP address of the device in the **Host Name/IP** field.
      – Use the default values for other parameters.
   d. Click **Configure** in the **SNMP Settings** area.

Figure 2 Adding the device



Resource > Add Device

Basic Information

Host Name/IP * 192.168.100.68

Device Label

Mask

Device Group

Login Type Telnet

☑ Automatically register to receive SNMP traps from supported devices

☑ Support Ping Operation

□ Add the device regardless of the ping result

□ Use the loopback address as the management IP

SNMP Settings

Configure

Parameter Type SNMPv2c

Read-Only Community String ******

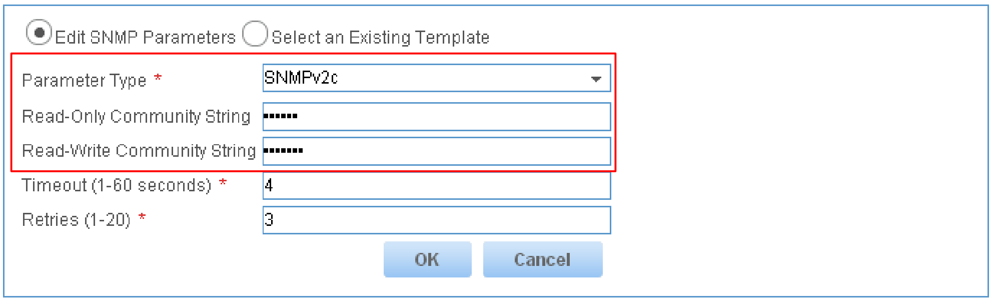
Read-Write Community String ******

Timeout (seconds) 4

Retries 3

3. Edit SNMP parameters:
   a. Select the **SNMPv2c** parameter type.
   b. Set the read-only community string to **readtest**.
   c. Set the read-write community string to **writetest**.
   d. Use the default values for other parameters.
   e. Click **OK**.

Figure 3 Configuring SNMP parameters



● Edit SNMP Parameters ○ Select an Existing Template

Parameter Type * SNMPv2c

Read-Only Community String ••••••

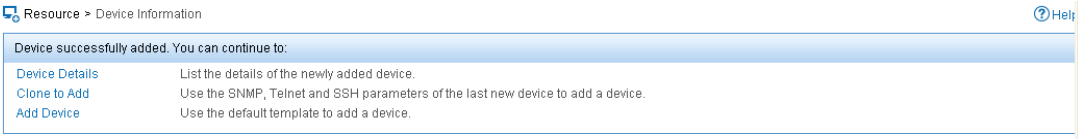
Read-Write Community String •••••••

Timeout (1-60 seconds) * 4

Retries (1-20) * 3

4. On the **Add Device** page, click **OK**. If the configuration succeeds, IMC returns a message as shown in Figure 4. Then you can monitor and manage the device from the IMC server.

Figure 4 Device adding success message



Resource > Device Information

Device successfully added. You can continue to:

Device Details List the details of the newly added device.

Clone to Add Use the SNMP, Telnet and SSH parameters of the last new device to add a device.

Add Device Use the default template to add a device.

Verifying the configuration

Verify that the device sends notifications to the NMS when the state of an interface changes:

1. Execute the **`shutdown`** or **`undo shutdown`** command on an idle interface to shut down or bring up the interface.
2. Navigate to the **Alarm** > **Alarm Browse** > **All Alarms** page on the IMC server to identify whether a notification about the interface state change exists.

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 securityname
readtest v2c
#
```

Related documentation

- SNMP configuration in the network management and monitoring configuration guide for the device.
- SNMP commands in the network management and monitoring command reference for the device.

Configuring SNMPv3

Introduction

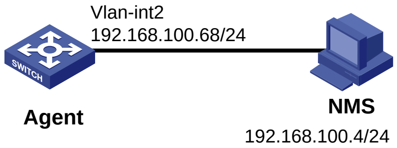
The following information uses an example to describe the basic SNMPv3 configuration procedure.

Network configuration

As shown in Figure 5, configure the device (agent) and IMC server (NMS) to meet the following requirements:

- Enable the IMC server to monitor and manage the device through SNMPv3 as an NMS.
- Enable the device to send notifications to report events to the NMS as an agent.
- Ensure secure communication between the NMS and device.

Figure 5 Network diagram



Restrictions and guidelines

- SNMPv3 supports view-based access control (VACM) and role-based access control (RBAC) models. This example provides the SNMPv3 configuration procedure in both access control models.
- Configure the same SNMP version and community string on the NMS and device to make sure the NMS can monitor and manage the device.
- The NMS configuration method varies by vendor. For information about configuring the NMS, see the manual for the NMS. This example uses the IMC PLAT 7.0 (E0202) NMS.
- The security name used for the NMS to receive SNMPv3 notifications must be an existing SNMPv3 username.
- The NMS and agent must use the same security model.
- The SNMPv3 authentication and encryption passwords are saved to the configuration file in encrypted form. An encrypted-form password is calculated from the plaintext-form password and the local engine ID. To configure the same authentication and encryption passwords for two devices, configure plaintext-form passwords manually on the two devices. Do not copy the encrypted-from passwords in the configuration file from one device to another. If you do so, you will get different plaintext-form passwords on the two devices because the two devices use different local engine IDs.

Procedure

Configuring the device

Configuring SNMPv3 settings in RBAC model

# Assign an IP address to VLAN-interface 2.

```
<Agent> system-view
[Agent] interface Vlan-interface2
[Agent-Vlan-interface2] ip address 192.168.100.68 24
[Agent-Vlan-interface2] quit
```

# Enable SNMPv3.

```
[Agent] snmp-agent sys-info version v3
```

# Create user role **test**, and assign **test** read and write access to the objects of 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 encryption key to **123456TESTencr&!** for the user.

```
[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 device.

```
[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 notifications target host and set the security name to **managev3user**.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

Configuring SNMPv3 settings in VACM model

# Assign an IP address to VLAN-interface 2.

```
<Agent> system-view
[Agent] interface Vlan-interface2
[Agent-Vlan-interface2] ip address 192.168.100.68 24
[Agent-Vlan-interface2] quit
```

# Enable SNMPv3.

```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```

# Create a MIB view named **midtest** to contain all objects in the **internet** subtree (OID 1.3.6.1).

```
[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&!** for the user.

```
[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 device.

```
[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
```

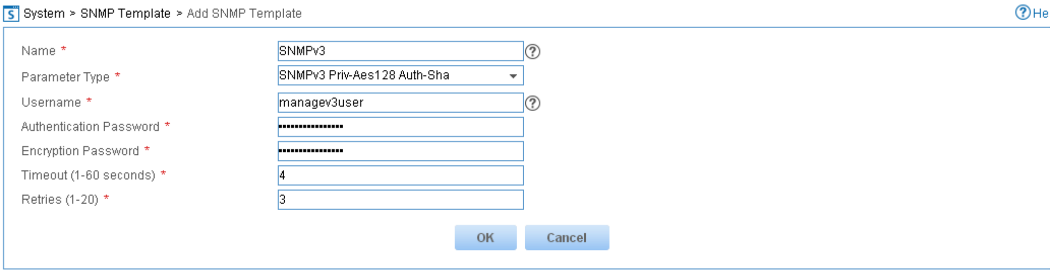
# Specify the NMS at **192.168.100.4** as the notifications target host and set the security name to **managev3user**.

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

Configuring the IMC server

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:
      – Set the SNMP template name to **SNMPv3**.
      – Select the **SNMPv3 Priv-Aes128 Auth-Sha** parameter type.
      – Set the username to **managev3user**.
      – Set the authentication password to **123456TESTauth&!** in plaintext form.
      – Set the encryption password to **123456TESTencr&!** in plaintext form.
      – Use the default values for other parameters.
      – Click **OK**.

Figure 6 Adding an SNMP template



System > SNMP Template > Add SNMP Template

Name * SNMPv3

Parameter Type * SNMPv3 Priv-Aes128 Auth-Sha

Username * managev3user

Authentication Password * ••••••••••••••••

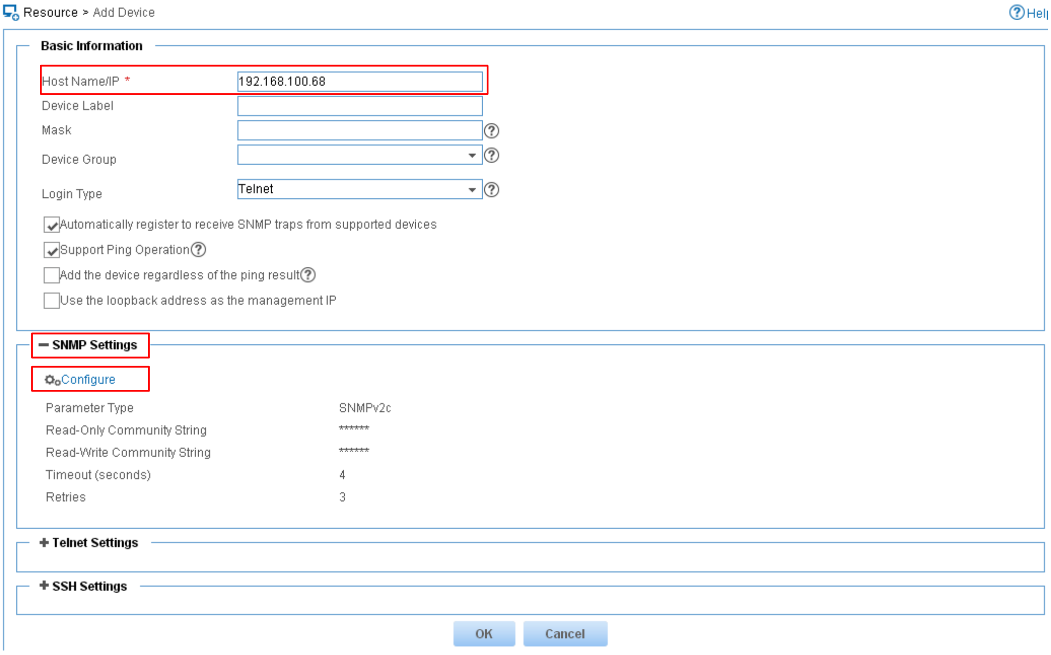
Encryption Password * ••••••••••••••••

Timeout (1-60 seconds) * 4

Retries (1-20) * 3

2. Add the device:
   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 the IP address or host name of the device in the **Host Name/IP** field.
      – Use the default values for other parameters.
   d. Click **Configure** in the **SNMP Settings** area.

Figure 7 Adding the device



Resource > Add Device

Basic Information

Host Name/IP *	192.168.100.68
Device Label	
Mask	
Device Group	
Login Type	Telnet

☑ Automatically register to receive SNMP traps from supported devices

☑ Support Ping Operation

□ Add the device regardless of the ping result

□ Use the loopback address as the management IP

SNMP Settings

Configure

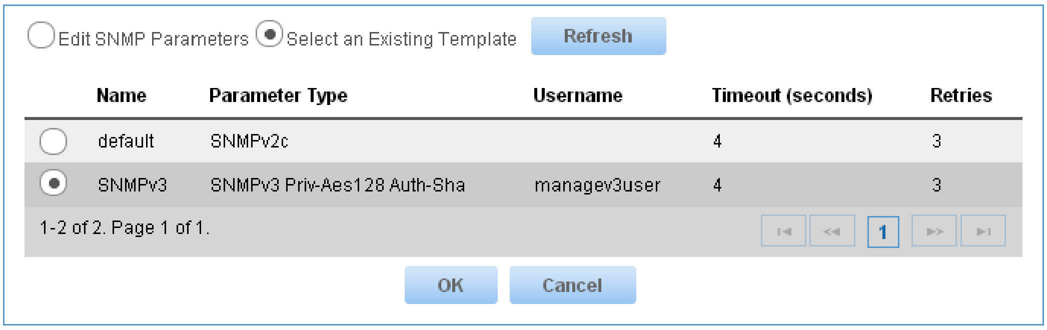
Parameter Type	SNMPv2c
Read-Only Community String	******
Read-Write Community String	******
Timeout (seconds)	4
Retries	3

Telnet Settings

SSH Settings

3. Edit SNMP parameters:
   a. Select the **Select an Existing Template** option.
   b. Select the SNMP template named **SNMPv3**.
   c. Click **OK**.

Figure 8 Selecting SNMP parameters



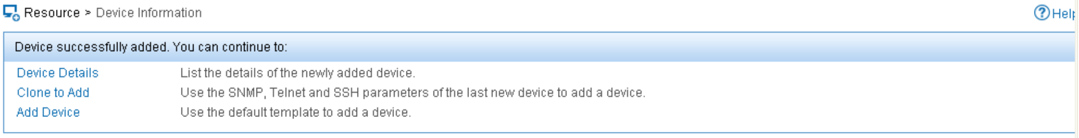
○ Edit SNMP Parameters ● Select an Existing Template

	Name	Parameter Type	Username	Timeout (seconds)	Retries
○	default	SNMPv2c		4	3
●	SNMPv3	SNMPv3 Priv-Aes128 Auth-Sha	managev3user	4	3

1-2 of 2. Page 1 of 1.

4. On the **Add Device** page, click **OK**. If the configuration succeeds, IMC returns a message as shown in Figure 9. Then you can monitor and manage the device from the IMC server.

Figure 9 Device added



Resource > Device Information

Device successfully added. You can continue to:

Device Details	List the details of the newly added device.
Clone to Add	Use the SNMP, Telnet and SSH parameters of the last new device to add a device.
Add Device	Use the default template to add a device.

Verifying the configuration

Verify that the device sends notifications to the NMS when the state of an interface changes:

1. Execute the **shutdown** or **undo shutdown** command on an idle interface to shut down or bring up the interface.
2. Navigate to the **Alarm** > **Alarm Browse** > **All Alarms** page on the IMC server to identify whether a notification about the interface state change exists..

Configuration files

- SNMPv3 settings in RBAC model

```
#
 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 write oid 1.3.6.1
#
```

- SNMPv3 settings in VACM model

```
#
 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==
#
```

Related documentation

- SNMP configuration in the network management and monitoring configuration guide for the device.
- SNMP commands in the network management and monitoring command reference for the device.

LAN Networks Quick Start Configuration Guide

Contents

Deploying a small-sized campus network ··· 1

Introduction ··· 1
Network configuration ··· 1
Analysis and data preparation ··· 2
Procedure ··· 4
Configuring the access switches ··· 4
Configuring the core switch ··· 8
Configuring the egress router ··· 12
Verifying the configuration ··· 13
Configuration files ··· 14
Related documentation ··· 17

Deploying a small- to medium-sized campus network ··· 19

Introduction ··· 19
Network configuration ··· 19
Analysis and data preparation ··· 20
Procedure ··· 22
Configuring the access switches ··· 22
Configuring the core switches ··· 25
Configuring the egress router ··· 31
Verifying the configuration ··· 36
Configuration files ··· 36
Related documentation ··· 40

Deploying a small-sized campus network

Introduction

The following information uses an example to describe the basic procedure for configuring a small-sized campus network.

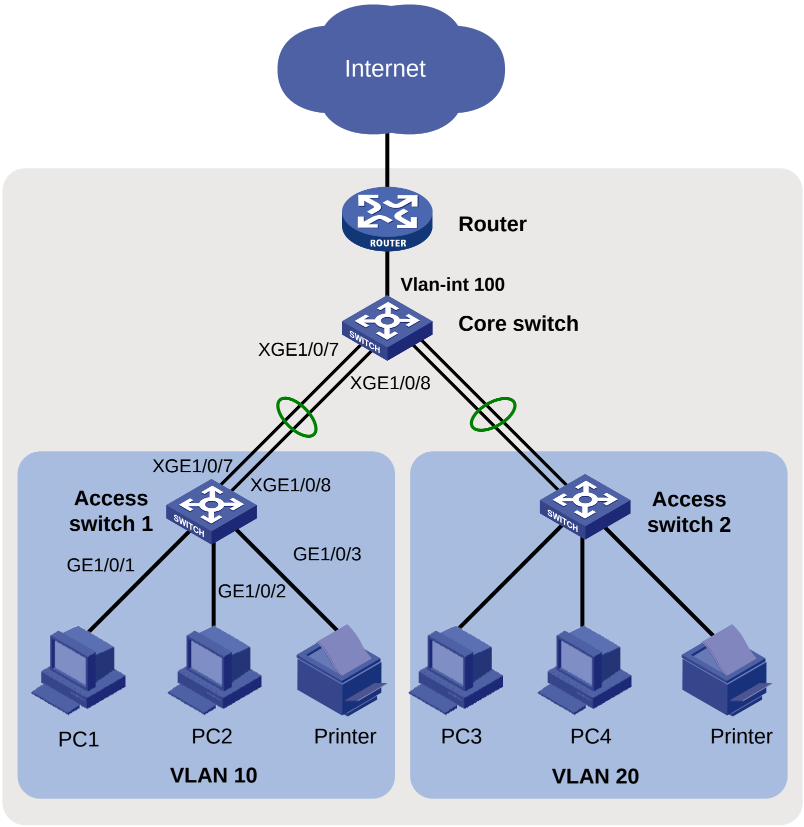
Network configuration

As shown in Figure 1, in a small-sized campus network, the S5130 or S5130S Ethernet switches series are deployed on the access layer. The S5560X or S6520X Ethernet switches series are deployed on the core layer, and an MSR series router is used as the egress router.

Configure the devices to meet the following requirements:

- Configure the spanning tree feature on all the switches to prevent loops.
- Configure link aggregation on the access switches and the core switch to provide high availability.
- Configure VLANs to accommodate services of different departments in the campus and configure VLAN interfaces to provide Layer 3 connectivity for inter-department services.
- Configure the core switch as the DHCP server to dynamically assign IP addresses to campus users.
- Enable DHCP snooping on the access switches to prevent unauthorized DHCP servers from assigning IP addresses to intranet users. Additionally, enable IPSG to prevent intranet users from changing their IP addresses.

Figure 1 Small-sized campus network diagram



Analysis and data preparation

Table 1 shows the procedure of deploying a small-sized campus network.

Table 1 Procedure of deploying a small-sized campus network

Step	Item	Configuration data	Remarks
1. Log in to the devices.	Console login	Communication parameters (the transmission rate, for example).	Use a PC to log in to the devices through a terminal emulation program.
2. Configure the management IP and Telnet login.	Management VLAN	VLAN 5	VLAN 1 is the default VLAN. Do not configure VLAN 1 as the management VLAN. This example uses VLAN 5 as the management VLAN.
	IP address of the management Ethernet interface or management VLAN interface	10.10.1.1/24	For a switch that has a management Ethernet interface, use the IP address of M-GigabitEthernet 0/0/0 for device login. For a switch that does not have a management Ethernet interface, use the IP address of the management VLAN interface for device

Step	Item	Configuration data	Remarks
			login.
3. Configure interfaces and VLANs.	Dynamic aggregation	- Access switch 1: Uplink aggregate interface Bridge-Aggregation 1 - Access switch 2: Uplink aggregate interface Bridge-Aggregation 1 - Core switch: Downlink aggregate interface Bridge-Aggregation 1	Access switches and the core switch are connected through aggregate links.
	Port link type	- Port connected to a PC: Access port - Port connected to a switch: Trunk port	N/A
	VLAN IDs	- Access switch 1: VLAN 10 - Access switch 2: VLAN 20 - Core switch: VLAN 100, VLAN 10, and VLAN 20	To isolate Department A and Department B at Layer 2, configure VLAN 10 for Department A and VLAN 20 for Department B. The core switch connects to the egress router through VLAN-interface 100.
4. Configure the DHCP server on the core switch.	DHCP server	N/A	N/A
	DHCP address pools	- VLAN 10: DHCP address pool 1 - VLAN 20: DHCP address pool 2	PCs in Department A and Department B obtain IP addresses from DHCP address pool 1 and DHCP address pool 2, respectively.
5. Configure routes on the core switch.	IP addresses	- VLAN-interface 10: 10.10.10.1/24 - VLAN-interface 20: 10.10.20.1/24 - VLAN-interface 100: 10.10.100.1/24	The core switch communicates with the egress router through VLAN-interface 100, which is used for the connectivity between the intranet and the egress router. You must configure a default route with the next hop as the egress router. Assign IP addresses to VLAN-interface 10 and VLAN-interface 20 to allow Department A and Department B to visit each other.
6. Configure the egress router.	IP address of the public network interface	GE0/2: 202.101.100.2/30	GE0/2 on the egress router is the public network interface that connects the router to the Internet.
	Public network	202.101.100.1/30	The egress router

Step	Item	Configuration data	Remarks
	gateway address		communicates with the service provider device through the public network gateway address. To forward intranet packets to the external network, you must configure a default route with the next hop as the public network gateway address.
	DNS server address	202.101.100.199	The DNS server translates domain names into IP addresses.
	IP address of the internal network interface	GE0/1: 10.10.100.2/24	GE0/1 on the egress router is the interface connected to the internal network.
7. Configure DHCP snooping on the access switches.	DHCP trusted port	N/A	Configure Bridge-Aggregation 1 as a DHCP trusted port.
8. Configure IPSG on the access switches.	IPSG	N/A	Configure IPv4SG to verify source IP address and source MAC address of user packets.

Procedure

Configuring the access switches

The procedure of configuring access switch 1 is the same as the procedure of configuring access switch 2. This section uses access switch 1 as an example.

1. Log in to the device through the console port (first device access):

# Shut down the PC from which you will log in to the device.

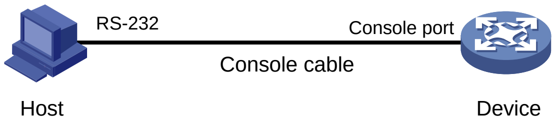
The serial ports on PCs do not support hot swapping. Before connecting a cable to or disconnecting a cable from a serial port on a PC, you must shut down the PC.

# Use the console cable shipped with the device to connect the PC to the console port of the device. Plug the DB-9 connector of the console cable into the 9-pin serial port of the PC, and then plug the RJ-45 connector into the console port of the device.

TIP:

- Identify interfaces correctly to avoid connection errors.
- To connect the PC to the device, first plug the DB-9 connector of the console cable into the 9-pin serial port of the PC, and then plug the RJ-45 connector of the console cable into the console port of the device.
- To disconnect the PC from the device, first unplug the RJ-45 connector and then the DB-9 connector.

Figure 2 Connecting a PC to the console port of the device



# Power on the PC, launch a terminal emulation program, and create a connection that uses the console port connected to the device. Set the port properties as follows:

- **Bits per second**—9600 bps.
- **Data bits**—8.
- **Stop bits**—1.
- **Parity**—None.
- **Flow control**—None.

# Power on the device and press **Enter** as prompted to enter the CLI.

# (Optional.) Configure the authentication mode for console login.

By default, authentication is disabled for console login. You can log in to the device without entering a username or password. To improve security, configure the authentication mode for console login after you log in to the device for the first time. For more information about authentication modes for console login, see login management configuration in *Fundamental Configuration Guide*.

2. Configure IP addresses and Telnet login:

# Create VLAN 5, and assign Ten-GigabitEthernet 1/0/10 (the port connected to the PC used for device login) to VLAN 5.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ACCSW1
[ACCSW1] vlan 5
[ACCSW1-vlan5] port ten-gigabitethernet 1/0/10
[ACCSW1-vlan5] quit
```

# Create VLAN-interface 5, and assign IP address 10.10.1.1/24 to it.

```
[ACCSW1] interface vlan-interface 5
[ACCSW1-Vlan-interface5] ip address 10.10.1.1 24
[ACCSW1-Vlan-interface5] quit
```

# Enable the Telnet service.

```
[ACCSW1] telnet server enable
```

# Enable scheme authentication for Telnet login.

```
[ACCSW1] line vty 0 63
[ACCSW1-line-vty0-63] authentication-mode scheme
[ACCSW1-line-vty0-63] quit
```

# Create local user **admin**. Set the password to **admin**, the service type to Telnet, and the user role to network-admin.

```
[ACCSW1] local-user admin
New local user added.
[ACCSW1-luser-manage-admin] password simple hello12345
[ACCSW1-luser-manage-admin] authorization-attribute user-role network-admin
[ACCSW1-luser-manage-admin] service-type telnet
[ACCSW1-luser-manage-admin] quit
```

# Telnet to the device from the PC by using the local user account **admin**.

The output varies by device model and software version. This example uses an S5560X-30C-PWR-EI switch running Release 1118P07.

```
C:\Users\Administrator> telnet 10.10.1.1
******************************************************************************
* 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.                    *
******************************************************************************

login: admin
Password:
<ACCSW1>
```

The output shows that you have Telneted to the device successfully.

3. Configure interfaces and VLANs:

# Create VLAN 10.

```
[ACCSW1] vlan 10
[ACCSW1-vlan10] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to PC 1) as an access port, assign it to VLAN 10, and configure it as an edge port.

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] port link-type access
[ACCSW1-GigabitEthernet1/0/1] port access vlan 10
[ACCSW1-GigabitEthernet1/0/1] stp edged-port
[ACCSW1-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to PC 2) as an access port, assign it to VLAN 10, and configure it as an edge port.

```
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] port link-type access
[ACCSW1-GigabitEthernet1/0/2] port access vlan 10
[ACCSW1-GigabitEthernet1/0/2] stp edged-port
[ACCSW1-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 (the port connected to the printer) as an access port, assign it to VLAN 10, and configure it as an edge port.

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] port link-type access
[ACCSW1-GigabitEthernet1/0/3] port access vlan 10
[ACCSW1-GigabitEthernet1/0/3] stp edged-port
[ACCSW1-GigabitEthernet1/0/3] quit
```

4. Configure link aggregation:

# Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] link-aggregation mode dynamic
[ACCSW1-Bridge-Aggregation1] quit
```

# Assign Ten-GigabitEthernet 1/0/7 and Ten-GigabitEthernet 1/0/8 to aggregation group 1.

```
[ACCSW1] interface ten-gigabitethernet 1/0/7
[ACCSW1-Ten-GigabitEthernet1/0/7] port link-aggregation group 1
[ACCSW1-Ten-GigabitEthernet1/0/7] quit
```

```
[ACCSW1] interface ten-gigabitethernet 1/0/8
[ACCSW1-Ten-GigabitEthernet1/0/8] port link-aggregation group 1
[ACCSW1-Ten-GigabitEthernet1/0/8] quit
```

# Configure Bridge-Aggregation 1 as a trunk port, and assign it to VLAN 10.

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] port link-type trunk
[ACCSW1-Bridge-Aggregation1] port trunk permit vlan 10
[ACCSW1-Bridge-Aggregation1] quit
```

# Display detailed information about Bridge-Aggregation 1 to verify the link aggregation configuration.

```
[ACCSW1] display link-aggregation verbose Bridge-Aggregation 1
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, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  XGE1/0/7            S        32768    61       2                      {ACDEF}
  XGE1/0/8            S        32768    62       2                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  XGE1/0/7(R)         32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  XGE1/0/8            32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
```

# Display information about VLAN 10 to verify the configuration.

```
[ACCSW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/1          GigabitEthernet1/0/2
    GigabitEthernet1/0/3          Ten-GigabitEthernet1/0/7
    Ten-GigabitEthernet1/0/8
```

5. Enable BPDU guard globally.

```
[ACCSW1] stp bpdu-protection
```

6. Configure DHCP snooping:

# Enable DHCP snooping.

```
[ACCSW1] dhcp snooping enable
```

# Configure Bridge-Aggregation 1 as a trusted port.

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] dhcp snooping trust
[ACCSW1-Bridge-Aggregation1] quit
```

7. Configure IPSG:

   # Enable IPv4SG on GigabitEthernet 1/0/1 and verify the source IPv4 address and MAC address for dynamic IPSG, and enable recording of client information in DHCP snooping entries on the interface.

   ```
   [ACCSW1] interface gigabitethernet 1/0/1
   [ACCSW1-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   [ACCSW1-GigabitEthernet1/0/1] dhcp snooping binding record
   [ACCSW1-GigabitEthernet1/0/1] quit
   ```

   # Enable IPv4SG on GigabitEthernet 1/0/2 and verify the source IPv4 address and MAC address for dynamic IPSG, and enable recording of client information in DHCP snooping entries on the interface.

   ```
   [ACCSW1] interface gigabitethernet 1/0/2
   [ACCSW1-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   [ACCSW1-GigabitEthernet1/0/2] dhcp snooping binding record
   [ACCSW1-GigabitEthernet1/0/2] quit
   ```

8. Save the configuration:

   # Save the running configuration on the access switches. This example uses access switch 1.

   ```
   [ACCSW1] 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.
   ```

Configuring the core switch

1. Log in to the device.

   For more information about logging in to the device, see "Log in to the device through the console port (first device access):."

2. Configure IP addresses and Telnet login.

   For more information about configuring IP addresses and Telnet login, see "Configure IP addresses and Telnet login:."

3. Configure VLANs and VLAN interfaces:

   # Create VLAN 10, VLAN 20, and VLAN 100.

   ```
   <Sysname> system-view
   [Sysname] sysname CORESW1
   [CORESW1] vlan 10 20
   [CORESW1] vlan 100
   [CORESW1-vlan100] port gigabitethernet 1/0/1
   [CORESW1-vlan100] quit
   ```

   # Create VLAN-interface 10, and assign IP address 10.10.10.1/24 to it.

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10]ip address 10.10.10.1 24
[CORESW1-Vlan-interface10] quit
```

# Create VLAN-interface 20, and assign IP address 10.10.20.1/24 to it.

```
[CORESW1] interface vlan-interface 20
[CORESW1-Vlan-interface20]ip address 10.10.20.1 24
[CORESW1-Vlan-interface20] quit
```

# Create VLAN-interface 100, and assign IP address 10.10.100.1/24 to it.

```
[CORESW1] interface vlan-interface 100
[CORESW1-Vlan-interface100]ip address 10.10.100.1 24
[CORESW1-Vlan-interface100] quit
```

4. Configure link aggregation:

# Create Layer 2 aggregate interface Bridge-Aggregation 1, and set the link aggregation mode to dynamic.

```
[CORESW1] interface bridge-aggregation 1
[CORESW1-Bridge-Aggregation1] link-aggregation mode dynamic
[CORESW1-Bridge-Aggregation1] quit
```

# Assign Ten-GigabitEthernet 1/0/7 and Ten-GigabitEthernet 1/0/8 to aggregation group 1.

```
[CORESW1] interface ten-gigabitethernet 1/0/7
[CORESW1-Ten-GigabitEthernet1/0/7] port link-aggregation group 1
[CORESW1-Ten-GigabitEthernet1/0/7] quit
[CORESW1] interface ten-gigabitethernet 1/0/8
[CORESW1-Ten-GigabitEthernet1/0/8] port link-aggregation group 1
[CORESW1-Ten-GigabitEthernet1/0/8] quit
```

# Configure Bridge-Aggregation 1 as a trunk port, and assign it to VLAN 10.

```
[CORESW1] interface bridge-aggregation 1
[CORESW1-Bridge-Aggregation1] port link-type trunk
[CORESW1-Bridge-Aggregation1] port trunk permit vlan 10
[CORESW1-Bridge-Aggregation1] quit
```

# Display detailed information about Bridge-Aggregation 1 to verify the link aggregation configuration.

```
[CORESW1] display link-aggregation verbose Bridge-Aggregation 1
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, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  XGE1/0/7(R)         S        32768    61       2                      {ACDEF}
  XGE1/0/8            S        32768    62       2                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  XGE1/0/7            32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  XGE1/0/8            32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
```

# Display information about VLAN 10 to verify the configuration.

```
[CORESW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.10.10.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Bridge-Aggregation1
    Ten-GigabitEthernet1/0/7      Ten-GigabitEthernet1/0/8
```

# Display information about VLAN 100 to verify the configuration.

```
[CORESW1] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.10.100.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:   None
 Untagged ports:   None
```

5. Configure the DHCP server feature:

# Enable DHCP.

```
[CORESW1] dhcp enable
```

# Create DHCP address pool 1. In this pool, specify network segment 10.10.10.0/24, gateway address 10.10.10.1, DNS server address 202.101.100.199, set the lease duration to 30 days, and bind IP address 10.10.10.254/24 to the printer.

```
[CORESW1] dhcp server ip-pool 1
[CORESW1-dhcp-pool-1] network 10.10.10.0 mask 255.255.255.0
[CORESW1-dhcp-pool-1] gateway-list 10.10.10.1
[CORESW1-dhcp-pool-1] dns-list 202.101.100.199
[CORESW1-dhcp-pool-1] expired day 30
[CORESW1-dhcp-pool-1] static-bind ip-address 10.10.10.254 24 client-identifier aabb-cccc-dd
[CORESW1-dhcp-pool-1] quit
```

# Create DHCP address pool 2. In this pool, specify network segment 10.10.20.0/24, gateway address 10.10.20.1, DNS server address 202.101.100.199, and set the lease duration to 30 days.

```
[CORESW1] dhcp server ip-pool 2
[CORESW1-dhcp-pool-2] network 10.10.20.0 mask 255.255.255.0
[CORESW1-dhcp-pool-2] gateway-list 10.10.20.1
```

```
[CORESW1-dhcp-pool-2] dns-list 202.101.100.199
[CORESW1-dhcp-pool-2] expired day 30
[CORESW1-dhcp-pool-2] quit
```

# Enable the DHCP server on VLAN-interface 10, and apply DHCP address pool 1 to VLAN-interface 10.

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] dhcp select server
[CORESW1-Vlan-interface10] dhcp server apply ip-pool 1
[CORESW1-Vlan-interface10] quit
```

# Enable the DHCP server on VLAN-interface 20, and apply DHCP address pool 2 to VLAN-interface 20.

```
[CORESW1 interface vlan-interface 20
[CORESW1-Vlan-interface20] dhcp select server
[CORESW1-Vlan-interface20] dhcp server apply ip-pool 2
[CORESW1-Vlan-interface20] quit
```

# Display information about DHCP address pools.

```
[CORESW1] display dhcp server pool
Pool name: 1
  Network: 10.10.10.0 mask 255.255.255.0
  dns-list 202.101.100.199
  expired 30 0 0 0
  gateway-list 10.10.10.1
  static bindings:
    ip-address 10.10.10.254 mask 255.255.255.0
      client-identifier aabb-cccc-dd
Pool name: 2
  Network: 10.10.20.0 mask 255.255.255.0
  dns-list 202.101.100.199
  expired 30 0 0 0
  gateway-list 10.10.20.1
```

6. Configure a static route and display routing table information:

# Configure a default static route with next hop 10.10.100.2 (the IP address of the router).

```
[CORESW1] ip route-static 0.0.0.0 0 10.10.100.2
```

# Display routing table information.

```
[CORESW1] display ip routing-table

Destinations : 21       Routes : 21

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/0          Static  60  0           10.10.100.2     Vlan100
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.10.10.0/24      Direct  0   0           10.10.10.1      Vlan10
10.10.10.0/32      Direct  0   0           10.10.10.1      Vlan10
10.10.10.1/32      Direct  0   0           127.0.0.1       InLoop0
10.10.10.255/32    Direct  0   0           10.10.10.1      Vlan10
10.10.20.0/24      Direct  0   0           10.10.20.1      Vlan20
10.10.20.0/32      Direct  0   0           10.10.20.1      Vlan20
10.10.20.1/32      Direct  0   0           127.0.0.1       InLoop0
```

```
10.10.20.255/32    Direct  0   0           10.10.20.1      Vlan20
10.10.100.0/24     Direct  0   0           10.10.100.1     Vlan100
10.10.100.0/32     Direct  0   0           10.10.100.1     Vlan100
10.10.100.1/32     Direct  0   0           127.0.0.1       InLoop0
10.10.100.255/32   Direct  0   0           10.10.100.1     Vlan100
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
```

7. Save the configuration:

   # Save the running configuration on the core switch.

   ```
   [CORESW1] 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.
   ```

Configuring the egress router

1. Log in to the router.

   For more information about logging in to the router, see "Log in to the device through the console port (first device access):."

2. Configure IP addresses and Telnet login.

   For more information about configuring IP addresses and Telnet login, see "Configure IP addresses and Telnet login:."

3. Assign IP addresses to the public network interface and the internal network interface:

   # Assign IP address 202.101.100.2/30 to GigabitEthernet 0/2 (the public network interface).

   ```
   [Router] interface GigabitEthernet 0/2
   [Router-GigabitEthernet0/2] ip address 202.101.100.2 30
   [Router-GigabitEthernet0/2] quit
   ```

   # Assign IP address 10.10.100.2/24 to GigabitEthernet 0/1 (the internal network interface).

   ```
   [Router] interface GigabitEthernet 0/1
   [Router-GigabitEthernet0/1] ip address 10.10.100.2 24
   [Router-GigabitEthernet0/1] quit
   ```

4. Configure packet filtering:

   # Configure ACL 2000.

   ```
   [Router] acl basic 2000
   [Router-acl-ipv4-basic-2000] rule permit source 10.10.10.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 10.10.20.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 10.10.100.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] quit
   ```

   # Apply ACL 2000 to GigabitEthernet 0/1 to filter incoming packets.

   ```
   [Router] interface gigabitethernet 0/1
   [Router-GigabitEthernet0/1] packet-filter 2000 inbound
   [Router-GigabitEthernet0/1] quit
   ```

# Set the packet filtering default action to deny.

```
[Router] packet-filter default deny
```

# Display configuration and match statistics for ACL 2000.

```
[Router] display acl 2000
Basic IPv4 ACL 2000, 3 rules,
ACL's step is 5, start ID is 0
 rule 0 permit source 10.10.10.0 0.0.0.255
 rule 5 permit source 10.10.20.0 0.0.0.255
 rule 10 permit source 10.10.100.0 0.0.0.255
```

# Display ACL application information for inbound packet filtering on GigabitEthernet 0/1.

```
[Router] display packet-filter interface gigabitethernet 0/1 inbound
Interface: GigabitEthernet 0/1
 Inbound policy:
  IPv4 ACL 2000
```

5. Configure static routes to the intranet and the public network:

   ```
   [Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
   [Router] ip route-static 10.10.20.0 255.255.255.0 10.10.100.1
   [Router] ip route-static 0.0.0.0 0.0.0.0 202.101.100.1
   ```

6. Configure DNS:

   ```
   [Router] dns server 202.101.100.199
   [Router] dns proxy enable
   ```

7. Save the configuration:

   # Save the running configuration on the egress router.

   ```
   [Router] 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.
   ```

Verifying the configuration

1. Verify that two PCs in the same department can ping each other. This example uses PC 1 and PC 2 in Department A.

   # Ping PC 2 from PC 1.

   ```
   <PC1> ping 10.10.10.20
   Ping 10.10.10.20 (10.10.10.20): 56 data bytes, press CTRL+C to break
   56 bytes from 10.10.10.20: icmp_seq=0 ttl=255 time=1.015 ms
   56 bytes from 10.10.10.20: icmp_seq=1 ttl=255 time=2.338 ms
   56 bytes from 10.10.10.20: icmp_seq=2 ttl=255 time=1.951 ms
   56 bytes from 10.10.10.20: icmp_seq=3 ttl=255 time=1.719 ms
   56 bytes from 10.10.10.20: icmp_seq=4 ttl=255 time=1.629 ms

   --- Ping statistics for 10.10.10.20 ---
   5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 1.015/1.730/2.338/0.434 ms
   ```

The output shows that PC 1 can ping PC 2.

2. Verify that two PCs in different departments can ping each other. This example uses PC 1 in Department A and PC 3 in Department B. Assume that PC3 obtains IP address 10.10.20.10 through DHCP.

   # Ping PC 3 from PC 1.

   ```
   <PC1> ping 10.10.20.10
   Ping 10.10.20.10 (10.10.20.10): 56 data bytes, press CTRL+C to break
   56 bytes from 10.10.20.10: icmp_seq=0 ttl=254 time=2.709 ms
   56 bytes from 10.10.20.10: icmp_seq=1 ttl=254 time=0.877 ms
   56 bytes from 10.10.20.10: icmp_seq=2 ttl=254 time=0.850 ms
   56 bytes from 10.10.20.10: icmp_seq=3 ttl=254 time=0.805 ms
   56 bytes from 10.10.20.10: icmp_seq=4 ttl=254 time=0.814 ms

   --- Ping statistics for 10.10.20.10 ---
   5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 0.805/1.211/2.709/0.749 ms
   ```

   The output shows that PC 1 can ping PC 3.

3. Verify that a PC in each department can ping the external network. This example uses PC 1 in Department A to ping the public network gateway address. (Details not shown.)

Configuration files

Access switch ACCSW1

```
#
 sysname ACCSW1
#
 telnet server enable
#
 dhcp snooping enable
#
vlan 5
#
vlan 10
#
 stp bpdu-protection
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
 dhcp snooping trust
#
interface Vlan-interface5
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
```

```
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
 stp edged-port
#
interface Ten-GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 5
#
line vty 0 63
 authentication-mode scheme
#
local-user admin class manage
 password hash
$h$6$/up8ijTTulpXAAkL$s9fFDXwWVzNd0j2F8Rq/ZQEiMbA2s8uW31kkcaDoGHoNyvE/zZLV9HoLp+i0+Vc
V6Jpm48ufEAxbuKvi6qtWmg==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

Access switch ACCSW2

The configuration file of ACCSW2 is the same as that of ACCSW1 except the VLAN IDs, management VLAN interface address, and aggregate interface number. (Details not shown.)

Core switch CORESW1

```
#
 sysname CORESW1
```

```
#
vlan 10
#
vlan 20
#
vlan 100
#
dhcp server ip-pool 1
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
 static-bind ip-address 10.10.10.254 mask 255.255.255.0 client-identifier aaaa-cccc-dd
#
dhcp server ip-pool 2
 gateway-list 10.10.20.1
 network 10.10.20.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
#
interface Vlan-interface10
 ip address 10.10.10.1 255.255.255.0
 dhcp server apply ip-pool 1
#
interface Vlan-interface20
 ip address 10.10.20.1 255.255.255.0
 dhcp server apply ip-pool 2
#
interface Vlan-interface100
 ip address 10.10.100.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
 ip route-static 0.0.0.0 0 10.10.100.2
#
```

Egress router

```
#
 sysname Router
#
 packet-filter default deny
#
 dns proxy enable
 dns server 202.101.100.199
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.10.100.2 255.255.255.0
 packet-filter 2000 inbound
#
interface GigabitEthernet0/2
 port link-mode route
 ip address 202.101.100.2 255.255.255.252
#
 ip route-static 0.0.0.0 0 202.101.100.1
 ip route-static 10.10.10.0 24 10.10.100.1
 ip route-static 10.10.20.0 24 10.10.100.1
#
acl basic 2000
 rule 0 permit source 10.10.10.0 0.0.0.255
 rule 5 permit source 10.10.20.0 0.0.0.255
 rule 10 permit source 10.10.100.0 0.0.0.255
#
```

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.
- VLAN configuration in the Layer 2—LAN switching configuration guide for the device.
- VLAN commands in the Layer 2—LAN switching command reference for the device.
- Ethernet link aggregation configuration in the Layer 2—LAN switching configuration guide for the device.
- Ethernet link aggregation commands in the Layer 2—LAN switching command reference for the device.
- DHCP configuration in the Layer 3—IP services configuration guide for the device.
- DHCP commands in the Layer 3—IP services command reference for the device.
- ACL configuration in the ACL and QoS configuration guide for the device.

- ACL commands in the ACL and QoS command reference for the device.
- IP source guard configuration in the security configuration guide for the device.
- IP source guard commands in the security command reference for the device.

Deploying a small- to medium-sized campus network

Introduction

The following information uses an example to describe the basic procedure for configuring a small- to medium-sized campus network.

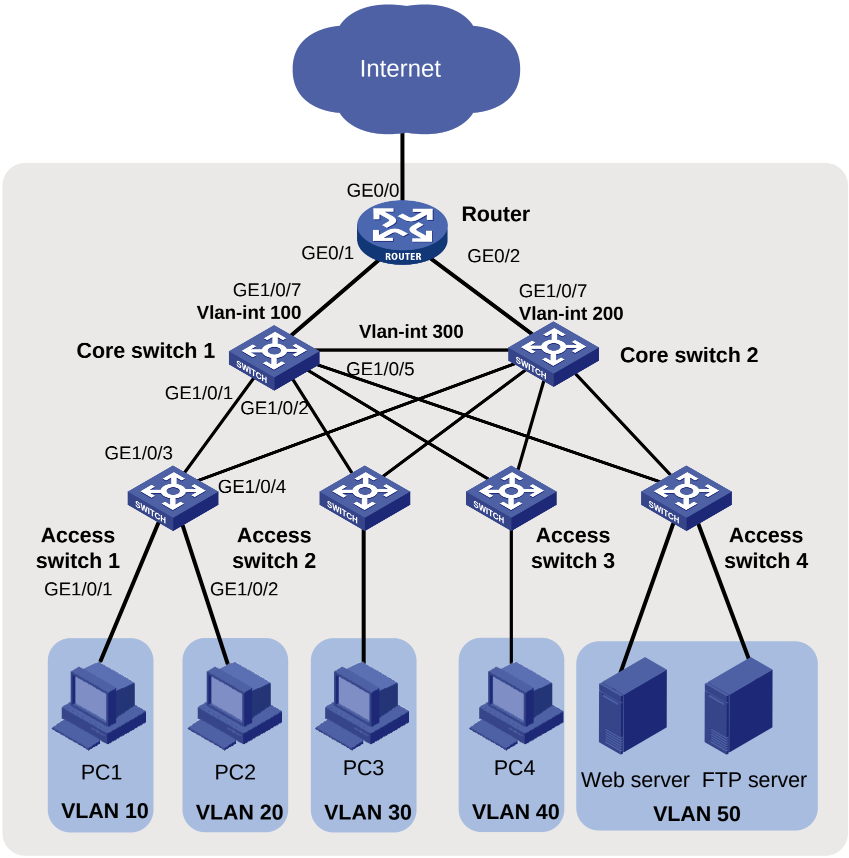
Network configuration

As shown in Figure 1, in a small- to medium-sized campus network, the S5130 or S5130S Ethernet switches series are deployed on the access layer. The S5560X or S6520X Ethernet switches series are deployed on the core layer, and an MSR series router is used as the egress router.

Configure the devices to meet the following requirements:

- Configure VRRP on the core switches to provide high availability.
- Configure VLANs to accommodate services of different departments and configure VLAN interfaces on the core switches to provide Layer 3 connectivity for inter-department services.
- Configure the core switches as the DHCP servers to dynamically assign IP addresses to campus users.
- Enable DHCP snooping on the access switches to prevent unauthorized DHCP servers from assigning IP addresses to intranet users. Additionally, enable IPSG to prevent intranet users from changing their IP addresses.
- Configure per-IP address rate liming on the egress router to limit the rate of incoming and outgoing traffic.

Figure 3 Small- to medium-sized campus network diagram



Analysis and data preparation

Table 2 shows the procedure of deploying a small-l to medium-sized campus network.

Table 2 Procedure of deploying a small- to medium-sized campus network

Step	Item	Configuration data	Remarks
1. Log in to the devices.	Console login	Communication parameters (the transmission rate, for example).	Use a PC to log in to the devices through a terminal emulation program.
2. Configure the management IP and Telnet login.	Management VLAN	VLAN 5	VLAN 1 is the default VLAN. Do not configure VLAN 1 as the management VLAN. This example uses VLAN 5 as the management VLAN.
	IP address of the management Ethernet interface or management VLAN interface	10.10.1.1/24	This example uses ACCSW1. For a switch that has a management Ethernet interface, use the IP address of M-GigabitEthernet 0/0/0 for device login. For a switch that does not have a management

Step	Item	Configuration data	Remarks
			Ethernet interface, use the IP address of the management VLAN interface for device login.
3. Configure interfaces and VLANs.	Port link type	• Port connected to a PC: Access or hybrid port • Port connected to a switch: Trunk or hybrid port	N/A
	VLAN IDs	• Access switch 1: VLANs 10 and 20 • Core switch: VLANs 10, 20, 30, 40, 50, 100, and 300	To isolate Department A and Department B at Layer 2, configure VLAN 10 for Department A and VLAN 20 for Department B. The core switch connects to the egress router through VLAN-interface 100.
4. Configure the DHCP server on the core switches.	DHCP server	Core switch 1 Core switch 2	Configure the DHCP server feature on core switch 1 and core switch 2.
	DHCP address pools	• VLAN 10: DHCP address pool 1 • VLAN 20: DHCP address pool 2	PCs in Department A and Department B obtain IP addresses from DHCP address pool 1 and DHCP address pool 2, respectively.
5. Configure routes on the core switches.	IP addresses	Core switch 1: • VLAN-interface 10: 192.168.10.1/24 • VLAN-interface 20: 192.168.20.1/24 • VLAN-interface 100: 172.16.1.1/24 • VLAN-interface 300: 172.16.3.1/24	VLAN-interface100 is used for the communication between core switch 1 and the egress router. VLAN-interface 300 is used for the communication between core switch 1 and core switch 2. Assign IP addresses to VLAN-interface 10 and VLAN-interface 20 to allow Department A and Department B to visit each other.
6. Configure the egress router.	IP address of the public network interface	GE0/0: 202.101.100.2/30	GE0/0 on the egress router is the public network interface that connects the router to the Internet.
	Public network gateway address	202.101.100.1/30	The egress router communicates with the service provider device through the public network gateway address. To forward intranet packets to the external network, you must configure a default route with the next hop as the public network gateway

Step	Item	Configuration data	Remarks
			address.
	DNS server address	202.101.100.199	The DNS server translates domain names into IP addresses.
	IP addresses of the internal network interfaces	GE0/1: 172.16.1.2/24 GE0/2: 172.16.2.2/24	GE0/1 and GE0/2 on the egress router are used for connection between the egress router and the intranet. The egress router connects to the master device and the backup device through GE0/1 and GE0/2, respectively.
7. Configure DHCP snooping and IP source guard on the access switches.	Trusted ports	GE1/0/1 GE1/0/2	A trusted port can forward DHCP messages correctly to ensure that the clients get IP addresses from authorized DHCP servers.

Procedure

Configuring the access switches

The procedure of configuring access switch 1 is the same as the procedure of configuring access switches 2, 3, and 4. This section uses access switch 1 as an example.

1. Log in to the device through the console port (first device access):

   # Shut down the PC from which you will log in to the device.

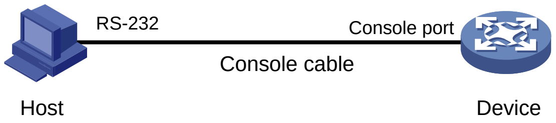
   The serial ports on PCs do not support hot swapping. Before connecting a cable to or disconnecting a cable from a serial port on a PC, you must shut down the PC.

   # Use the console cable shipped with the device to connect the PC to the console port of the device. Plug the DB-9 connector of the console cable into the 9-pin serial port of the PC, and then plug the RJ-45 connector into the console port of the device.

TIP:

- Identify interfaces correctly to avoid connection errors.
- To connect the PC to the device, first plug the DB-9 connector of the console cable into the 9-pin serial port of the PC, and then plug the RJ-45 connector of the console cable into the console port of the device.
- To disconnect the PC from the device, first unplug the RJ-45 connector and then the DB-9 connector.

Figure 4 Connecting a PC to the console port of the device



# Power on the PC, launch a terminal emulation program, and create a connection that uses the console port connected to the device. Set the port properties as follows:

- **Bits per second**—9600 bps.
- **Data bits**—8.
- **Stop bits**—1.
- **Parity**—None.
- **Flow control**—None.

# Power on the device and press **Enter** as prompted to enter the CLI.

# (Optional.) Configure the authentication mode for console login.

By default, authentication is disabled for console login. You can log in to the device without entering a username or password. To improve security, configure the authentication mode for console login after you log in to the device for the first time. For more information about authentication modes for console login, see login management configuration in *Fundamental Configuration Guide*.

2. Configure IP addresses and Telnet login:

# Create VLAN 5, and assign Ten-GigabitEthernet 1/0/10 (the port connected to the PC used for device login) to VLAN 5.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ACCSW1
[ACCSW1] vlan 5
[ACCSW1-vlan5] port ten-gigabitethernet 1/0/10
[ACCSW1-vlan5] quit
```

# Create VLAN-interface 5, and assign IP address 10.10.1.1/24 to it.

```
[ACCSW1] interface vlan-interface 5
[ACCSW1-Vlan-interface5] ip address 10.10.1.1 24
[ACCSW1-Vlan-interface5] quit
```

# Enable the Telnet service.

```
[ACCSW1] telnet server enable
```

# Enable scheme authentication for Telnet login.

```
[ACCSW1] line vty 0 63
[ACCSW1-line-vty0-63] authentication-mode scheme
[ACCSW1-line-vty0-63] quit
```

# Create local user **admin**. Set the password to **admin**, the service type to Telnet, and the user role to network-admin.

```
[ACCSW1] local-user admin
New local user added.
[ACCSW1-luser-manage-admin] password simple hello12345
[ACCSW1-luser-manage-admin] authorization-attribute user-role network-admin
[ACCSW1-luser-manage-admin] service-type telnet
[ACCSW1-luser-manage-admin] quit
```

# Telnet to the device from the PC by using the local user account **admin**.

The output varies by device model and software version. This example uses an S5560X-30C-PWR-EI switch running Release 1118P07.

```
C:\Users\Administrator> telnet 10.10.1.1
******************************************************************************
* 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.                    *
******************************************************************************

login: admin
Password:
<ACCSW1>
```

The output shows that you have Telneted to the device successfully.

3. Configure interfaces and VLANs:

# Create VLAN 10 and VLAN 20.

```
[ACCSW1] vlan 10 20
```

# Configure GigabitEthernet 1/0/1 (the port connected to PC 1) as an access port, assign it to VLAN 10, and configure it as an edge port.

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] port link-type access
[ACCSW1-GigabitEthernet1/0/1] port access vlan 10
[ACCSW1-GigabitEthernet1/0/1] stp edged-port
[ACCSW1-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to PC 2) as an access port, assign it to VLAN 20, and configure it as an edge port.

```
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] port link-type access
[ACCSW1-GigabitEthernet1/0/2] port access vlan 20
[ACCSW1-GigabitEthernet1/0/2] stp edged-port
[ACCSW1-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 10 and VLAN 20.

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] port link-type trunk
[ACCSW1-GigabitEthernet1/0/3] port trunk permit vlan 10 20
[ACCSW1-GigabitEthernet1/0/3] quit
```

# Configure GigabitEthernet 1/0/4 as a trunk port, and assign it to VLAN 10 and VLAN 20.

```
[ACCSW1] interface gigabitethernet 1/0/4
[ACCSW1-GigabitEthernet1/0/4] port link-type trunk
[ACCSW1-GigabitEthernet1/0/4] port trunk permit vlan 10 20
[ACCSW1-GigabitEthernet1/0/4] quit
```

# Display information about VLAN 10.

```
[ACCSW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4
 Untagged ports:
    GigabitEthernet1/0/1
```

# Display information about VLAN 20.

```
[ACCSW1] display vlan 20
```

```
 VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4
 Untagged ports:
    GigabitEthernet1/0/2
```

4. Enable BPDU guard globally.

```
[ACCSW1] stp bpdu-protection
```

5. Configure DHCP snooping:

   # Enable DHCP snooping.

```
[ACCSW1] dhcp snooping enable
```

   # Configure GigabitEthernet 1/0/3 as a trusted port.

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] dhcp snooping trust
[ACCSW1-GigabitEthernet1/0/3] quit
```

6. Configure IPSG:

   # Enable IPv4SG on GigabitEthernet 1/0/1 and verify the source IPv4 address and MAC address for dynamic IPSG, and enable recording of client information in DHCP snooping entries on the interface.

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/1] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/1] quit
```

   # Enable IPv4SG on GigabitEthernet 1/0/2 and verify the source IPv4 address and MAC address for dynamic IPSG, and enable recording of client information in DHCP snooping entries on the interface.

```
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/2] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/2] quit
```

7. Save the configuration:

   # Save the running configuration on the access switches. This example uses access switch 1.

```
[ACCSW1] 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.
```

Configuring the core switches

The procedure of configuring core switch 1 is similar to the procedure of configuring core switch 2. This section uses core switch 1 as an example. Unless otherwise stated, the configuration of core switch 2 is the same as that of core switch 1.

1. Configure interfaces and VLANs:

   # Create VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 50, VLAN 100, and VLAN 300.

   ```
   <Sysname> system-view
   [Sysname] sysname CORESW1
   [CORESW1] vlan 10 20 30 40 50 100 300
   ```

   # Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 10 and VLAN 20.

   ```
   [CORESW1] interface gigabitethernet 1/0/1
   [CORESW1-GigabitEthernet1/0/1] port link-type trunk
   [CORESW1-GigabitEthernet1/0/1] port trunk permit vlan 10 20
   [CORESW1-GigabitEthernet1/0/1] quit
   ```

   # Configure GigabitEthernet 1/0/5 as a trunk port, and assign it to VLAN 300.

   ```
   [CORESW1] interface gigabitethernet 1/0/5
   [CORESW1-GigabitEthernet1/0/5] port link-type trunk
   [CORESW1-GigabitEthernet1/0/5] port trunk permit vlan 300
   [CORESW1-GigabitEthernet1/0/5] quit
   ```

   # Configure the link type and permit VLANs for other interfaces in a similar way. (Details not shown.)

2. Configure VLAN interfaces:

   # Create VLAN-interface 10, and assign IP address 192.168.10.1/24 to it.

   ```
   [CORESW1] interface vlan-interface 10
   [CORESW1-Vlan-interface10]ip address 192.168.10.1 24
   [CORESW1-Vlan-interface10] quit
   ```

   # Create VLAN-interface 20, and assign IP address 92.168.20.1/24 to it.

   ```
   [CORESW1] interface vlan-interface 20
   [CORESW1-Vlan-interface20]ip address 192.168.20.1 24
   [CORESW1-Vlan-interface20] quit
   ```

   # Create VLAN-interface 100, and assign IP address 172.16.1.1/24 to it.

   ```
   [CORESW1] interface vlan-interface 100
   [CORESW1-Vlan-interface100]ip address 172.16.1.1 24
   [CORESW1-Vlan-interface100] quit
   ```

   # Create VLAN-interface 300, and assign IP address 172.16.3.1/24 to it.

   ```
   [CORESW1] interface vlan-interface 300
   [CORESW1-Vlan-interface300]ip address 172.16.3.1 24
   [CORESW1-Vlan-interface300] quit
   ```

   # Create other VLAN interfaces and assign IP addresses to them in a similar way. (Details not shown.)

   # Display information about VLAN 10.

   ```
   [CORESW1] display vlan 10
    VLAN ID: 10
    VLAN type: Static
    Route interface: Configured
    IPv4 address: 192.168.10.1
    IPv4 subnet mask: 255.255.255.0
    Description: VLAN 0010
    Name: VLAN 0010
    Tagged ports:
       GigabitEthernet1/0/1
    Untagged ports:   None
   ```

# Display information about VLAN 20.

```
[CORESW1] display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.20.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/2
 Untagged ports:   None
```

# Display information about VLAN 100.

```
[CORESW1] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:   None
 Untagged ports:   None
```

# Display information about VLAN 300.

```
[CORESW1] display vlan 300
 VLAN ID: 300
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.3.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0300
 Name: VLAN 0300
 Tagged ports:
    GigabitEthernet1/0/5
 Untagged ports:   None
```

3. Configure VRRP:

Use core switch 1 and core switch 2 to form a VRRP group. Core switch 1 operates as the master to process intranet packets. When core switch 1 fails or the upstream link of core switch 1 fails, core switch 2 takes over to process intranet packets.

# On core switch 1, create VRRP group 1 and set its virtual IP address to 172.16.3.10.

```
[CORESW1] interface vlan-interface 300
[CORESW1-Vlan-interface300] vrrp vrid 1 virtual-ip 172.16.3.10
```

# Assign core switch 1 a higher priority than core switch 2 in VRRP group 1, so core switch 1 can become the master.

```
[CORESW1-Vlan-interface300] vrrp vrid 1 priority 120
```

# Configure core switch 1 to operate in preemptive mode, so it can become the master whenever it operates correctly. Set the preemption delay to 5000 centiseconds to avoid frequent status switchover.

```
[CORESW1-Vlan-interface300] vrrp vrid 1 preempt-mode delay 5000
```

```
[CORESW1-Vlan-interface300] quit
```

# Create track entry 1 to monitor the upstream link status of GigabitEthernet 1/0/7. When the upstream link fails, the track entry transits to Negative.

```
[CORESW1] track 1 interface gigabitethernet 1/0/7
[CORESW1-track-1] quit
```

# Configure the VFs in VRRP group 1 to monitor track entry 1, and decrease their weights by 30 when the track entry transits to Negative.

```
[CORESW1] interface vlan-interface 300
[CORESW1-Vlan-interface300] vrrp vrid 1 track 1 priority reduced 30
```

# On core switch 2, create VRRP group 1 and set its virtual IP address to 172.16.3.10.

```
<Sysname> system-view
[Sysname] sysname CORESW2
[CORESW2] interface vlan-interface 300
[CORESW2-Vlan-interface300] vrrp vrid 1 virtual-ip 172.16.3.10
```

# Set the priority of core switch 2 to 100 in VRRP group 1.

```
[CORESW2-Vlan-interface300] vrrp vrid 1 priority 100
```

# Configure core switch 2 to operate in preemptive mode, and set the preemption delay to 5000 centiseconds.

```
[CORESW2-Vlan-interface300] vrrp vrid 1 preempt-mode delay 5000
[CORESW2-Vlan-interface300] quit
```

# Display detailed information about VRRP group 1 on core switch 1.

```
[CORESW1] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface300
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Master
     Config Pri       : 120                Running Pri  : 120
     Preempt Mode     : Yes                Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 172.16.3.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 172.16.3.1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 30
```

# Display detailed information about VRRP group 1 on core switch 2.

```
[CORESW2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface300
     VRID             : 1                  Adver Timer  : 100
     Admin Status     : Up                 State        : Backup
     Config Pri       : 100                Running Pri  : 100
     Preempt Mode     : Yes                Delay Time   : 5000
     Become Master    : 27810ms left
     Auth Type        : None
     Virtual IP       : 172.16.3.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 172.16.3.1
```

The output shows that core switch 1 is operating as the master and core switch 2 is operating as the backup in VRRP group 1.

4. Configure the DHCP server feature:

# Enable DHCP.

```
[CORESW1] dhcp enable
```

# Create DHCP address pool 1. In this pool, specify network segment 192.168.10.0/24, gateway address 192.168.10.1, DNS server address 202.101.100.199, set the lease duration to 30 days, and bind IP address 192.168.10.254/24 to the printer.

```
[CORESW1] dhcp server ip-pool 1
[CORESW1-dhcp-pool-1] network 192.168.10.0 mask 255.255.255.0
[CORESW1-dhcp-pool-1] gateway-list 192.168.10.1
[CORESW1-dhcp-pool-1] dns-list 202.101.100.199
[CORESW1-dhcp-pool-1] expired day 30
[CORESW1-dhcp-pool-1] static-bind ip-address 192.168.10.254 24 client-identifier
aabb-cccc-dd
[CORESW1-dhcp-pool-1] quit
```

# Create DHCP address pool 2. In this pool, specify network segment 192.168.20.0/24, gateway address 192.168.20.1, DNS server address 202.101.100.199, and set the lease duration to 30 days.

# Configure DHCP address pool 2 to assign IP addresses and other configuration parameters to clients on subnet 192.168.10.0/24.

```
[CORESW1] dhcp server ip-pool 2
[CORESW1-dhcp-pool-2] network 192.168.20.0 mask 255.255.255.0
[CORESW1-dhcp-pool-2] gateway-list 192.168.20.1
[CORESW1-dhcp-pool-2] dns-list 202.101.100.199
[CORESW1-dhcp-pool-2] expired day 30
[CORESW1-dhcp-pool-2] quit
```

# Enable the DHCP server on VLAN-interface 10, and apply DHCP address pool 1 to VLAN-interface 10.

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] dhcp select server
[CORESW1-Vlan-interface10] dhcp server apply ip-pool 1
[CORESW1-Vlan-interface10] quit
```

# Enable the DHCP server on VLAN-interface 20, and apply DHCP address pool 2 to VLAN-interface 10.

```
[CORESW1 interface vlan-interface 20
[CORESW1-Vlan-interface20] dhcp select server
[CORESW1-Vlan-interface20] dhcp server apply ip-pool 2
[CORESW1-Vlan-interface20] quit
```

# Display DHCP address pool information.

```
[CORESW1] display dhcp server pool
Pool name: 1
  Network: 192.168.10.0 mask 255.255.255.0
  expired 30 0 0 0
  gateway-list 192.168.10.1
  static bindings:
    ip-address 192.168.10.254 mask 255.255.255.0
      client-identifier aabb-cccc-dd
Pool name: 2
  Network: 192.168.20.0 mask 255.255.255.0
  expired 30 0 0 0
  gateway-list 192.168.20.1
```

5. Configure OSPF:

   # Configure OSPF on core switch 1.

   ```
   [CORESW1] ospf 100 router-id 2.2.2.2
   [CORESW1-ospf-100] area 0
   [CORESW1-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255
   [CORESW1-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
   [CORESW1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
   [CORESW1-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
   [CORESW1-ospf-100-area-0.0.0.0] quit
   [CORESW1-ospf-100] quit
   ```

   # Configure OSPF on core switch 2.

   ```
   [CORESW2] ospf 100 router-id 3.3.3.3
   [CORESW2-ospf-100] area 0
   [CORESW2-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255
   [CORESW2-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
   [CORESW2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
   [CORESW2-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
   [CORESW2-ospf-100-area-0.0.0.0] quit
   [CORESW2-ospf-100] quit
   ```

   # Display OSPF neighbor information on core switch 1.

   ```
   [CORESW1] display ospf peer

            OSPF Process 100 with Router ID 2.2.2.2
                  Neighbor Brief Information

    Area: 0.0.0.0
    Router ID       Address         Pri Dead-Time  State             Interface
    3.3.3.3         172.16.3.2      1   33         Full/DR           Vlan300
   ```

   # Display OSPF neighbor information on core switch 2.

   ```
   [CORESW2] display ospf peer

            OSPF Process 100 with Router ID 3.3.3.3
                  Neighbor Brief Information

    Area: 0.0.0.0
    Router ID       Address         Pri Dead-Time  State             Interface
    2.2.2.2         172.16.3.1      1   36         Full/BDR          Vlan300
   ```

6. Save the configuration:

   # Save the running configuration on the core switches. This example uses core switch CORESW1.

   ```
   [CORESW1] 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.
```

Configuring the egress router

1. Assign IP addresses to the public network interfaces and the internal network interface:

   # Assign IP addresses to internet network interfaces.

   ```
   [Router] interface GigabitEthernet 0/1
   [Router-GigabitEthernet0/1] ip address 172.16.1.2 24
   [Router-GigabitEthernet0/1] quit
   [Router] interface GigabitEthernet 0/2
   [Router-GigabitEthernet0/2] ip address 172.16.2.2 24
   [Router-GigabitEthernet0/2] quit
   ```

   # Assign an IP address to the public network interface.

   ```
   [Router] interface GigabitEthernet 0/0
   [Router-GigabitEthernet0/0] ip address 202.101.100.2 30
   [Router-GigabitEthernet0/0] quit
   ```

2. Configure packet filtering:

   # Configure ACL 2000.

   ```
   [Router] acl basic 2000
   [Router-acl-ipv4-basic-2000] rule permit source 192.168.10.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 192.168.20.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 172.16.1.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 172.16.2.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] rule permit source 172.16.3.0 0.0.0.255
   [Router-acl-ipv4-basic-2000] quit
   ```

   # Apply ACL 2000 to GigabitEthernet 0/1 and GigabitEthernet 1/0/2 to filter incoming packets.

   ```
   [Router] interface gigabitethernet 0/1
   [Router-GigabitEthernet0/1] packet-filter 2000 inbound
   [Router-GigabitEthernet0/1] quit
   [Router] interface gigabitethernet 0/2
   [Router-GigabitEthernet0/2] packet-filter 2000 inbound
   [Router-GigabitEthernet0/2] quit
   ```

   # Set the packet filtering default action to deny.

   ```
   [Router] packet-filter default deny
   ```

   # Display configuration and match statistics for ACL 2000.

   ```
   [Router] display acl 2000
   Basic IPv4 ACL 2000, 5 rules,
   ACL's step is 5, start ID is 0
    rule 0 permit source 192.168.10.0 0.0.0.255
    rule 5 permit source 192.168.20.0 0.0.0.255
    rule 10 permit source 172.16.1.0 0.0.0.255
    rule 15 permit source 172.16.2.0 0.0.0.255
    rule 20 permit source 172.16.3.0 0.0.0.255
   ```

   # Display ACL application information for inbound packet filtering on GigabitEthernet 0/1.

```
[Router] display packet-filter interface gigabitethernet 0/1 inbound
Interface: GigabitEthernet0/1
 Inbound policy:
  IPv4 ACL 2000
```

# Display ACL application information for inbound packet filtering on GigabitEthernet 0/2.

```
[Router] display packet-filter interface gigabitethernet 0/2 inbound
Interface: GigabitEthernet0/2
 Inbound policy:
  IPv4 ACL 2000
```

3. Configure OSPF:

# Configure a default static route, whose next hop address is 202.101.100.1 (the public network gateway address).

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.100.1
```

# Configure OSPF and redistribute a default route into the OSPF routing domain.

```
[Router] ospf 10 router-id 1.1.1.1
[Router-ospf-10] default-route-advertise always
[Router-ospf-10] area 0
[Router-ospf-10-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] quit
[Router-ospf-10] quit
```

# Display OSPF neighbor information on the egress router.

```
[Router] display ospf peer

         OSPF Process 100 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         172.16.1.1      1   31         Full/DR           GE0/1
 3.3.3.3         172.16.2.1      1   39         Full/BDR          GE0/2
```

# Display OSPF neighbor information on core switch 1.

```
[CORESW1] display ospf routing

         OSPF Process 100 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 172.16.1.0/24      1        Transit 0.0.0.0         2.2.2.2         0.0.0.0
 172.16.2.0/24      2        Transit 172.16.3.2      1.1.1.1         0.0.0.0
 172.16.2.0/24      2        Transit 172.16.1.2      1.1.1.1         0.0.0.0
 172.16.3.0/24      1        Transit 0.0.0.0         3.3.3.3         0.0.0.0

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 0.0.0.0/0          1        Type2   1           172.16.1.2      1.1.1.1

 Total nets: 5
 Intra area: 4  Inter area: 0  ASE: 1  NSSA: 0
```

# Display OSPF neighbor information on core switch 2.

```
[CORESW2] display ospf routing

         OSPF Process 100 with Router ID 3.3.3.3
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 172.16.1.0/24      2        Transit 172.16.3.1      2.2.2.2         0.0.0.0
 172.16.1.0/24      2        Transit 172.16.2.2      2.2.2.2         0.0.0.0
 172.16.2.0/24      1        Transit 0.0.0.0         1.1.1.1         0.0.0.0
 172.16.3.0/24      1        Transit 0.0.0.0         3.3.3.3         0.0.0.0

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 0.0.0.0/0          1        Type2   1           172.16.2.2      1.1.1.1

 Total nets: 5
 Intra area: 4  Inter area: 0  ASE: 1  NSSA: 0
```

4. Configure DNS:

# Specify DNS server IPv4 address 202.101.100.199.

```
[Router] dns server 202.101.100.199
```

# Enable DNS proxy.

```
[Router] dns proxy enable
```

5. Configure per-IP-address rate limiting:

# Configure CAR lists.

```
[Router] qos carl 1 source-ip-address range 192.168.10.1 to 192.168.10.254
per-address shared-bandwidth
[Router] qos carl 2 source-ip-address range 192.168.20.1 to 192.168.20.254
per-address shared-bandwidth
[Router] qos carl 3 destination-ip-address range 192.168.10.1 to 192.168.10.254
per-address shared-bandwidth
[Router] qos carl 4 destination-ip-address range 192.168.20.1 to 192.168.20.254
per-address shared-bandwidth
```

# Configure CAR-list-based traffic policing.

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] qos car inbound carl 1 cir 512
[Router-GigabitEthernet0/1] qos car inbound carl 2 cir 512
[Router-GigabitEthernet0/1] qos car outbound carl 3 cir 512
[Router-GigabitEthernet0/1] qos car outbound carl 4 cir 512
[Router-GigabitEthernet0/1] quit
[Router] interface gigabitethernet 0/2
```

```
[Router-GigabitEthernet0/2] qos car inbound carl 1 cir 512
[Router-GigabitEthernet0/2] qos car inbound carl 2 cir 512
[Router-GigabitEthernet0/2] qos car outbound carl 3 cir 512
[Router-GigabitEthernet0/2] qos car outbound carl 4 cir 512
[Router-GigabitEthernet0/2] quit
```

# Display CAR list information.

```
[Router] display qos carl
List  Rules
1     source-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
2     source-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
3     destination-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
4     destination-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
```

# Display CAR configuration and statistics on GigabitEthernet 0/1.

```
[Router] display qos car interface gigabitethernet 0/1
Interface: GigabitEthernet0/1
 Direction: inbound
  Rule: If-match carl 1
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 2
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
 Direction: outbound
  Rule: If-match carl 3
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 4
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
```

# Display CAR configuration and statistics on GigabitEthernet 0/2.

```
[Router] display qos car interface gigabitethernet 0/2
Interface: GigabitEthernet0/2
 Direction: inbound
  Rule: If-match carl 1
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 2
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
 Direction: outbound
  Rule: If-match carl 3
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 4
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
```

6. Save the configuration:

# Save the running configuration on the egress router.

```
[Router] 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.
```

Verifying the configuration

1. Verify that two PCs in the same department can ping each other.

   # Use PC 1 in VLAN 10 to ping another PC in this VLAN.

   ```
   <PC1> ping 192.168.10.83
   Ping 192.168.10.83 (192.168.10.83): 56 data bytes, press CTRL+C to break
   56 bytes from 192.168.10.83: icmp_seq=0 ttl=255 time=1.328 ms
   56 bytes from 192.168.10.83: icmp_seq=1 ttl=255 time=0.808 ms
   56 bytes from 192.168.10.83: icmp_seq=2 ttl=255 time=0.832 ms
   56 bytes from 192.168.10.83: icmp_seq=3 ttl=255 time=0.904 ms
   56 bytes from 192.168.10.83: icmp_seq=4 ttl=255 time=0.787 ms

   --- Ping statistics for 192.168.10.83 ---
   5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 0.787/0.932/1.328/0.202 ms
   ```

2. Verify that two PCs in different departments can ping each other.

   # Use PC 1 in VLAN 10 to ping a PC in a different VLAN.

   ```
   <PC1> ping 192.168.20.5
   Ping 192.168.20.5 (192.168.20.5): 56 data bytes, press CTRL+C to break
   56 bytes from 192.168.20.5: icmp_seq=0 ttl=255 time=69.146 ms
   56 bytes from 192.168.20.5: icmp_seq=1 ttl=255 time=1.735 ms
   56 bytes from 192.168.20.5: icmp_seq=2 ttl=255 time=1.356 ms
   56 bytes from 192.168.20.5: icmp_seq=3 ttl=255 time=1.302 ms
   56 bytes from 192.168.20.5: icmp_seq=4 ttl=255 time=1.379 ms

   --- Ping statistics for 192.168.20.5 ---
   5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
   round-trip min/avg/max/std-dev = 1.302/14.984/69.146/27.082 ms
   ```

3. Verify that a PC in each department can ping the external network.

   # Use PC 1 in VLAN 10 to ping the public network gateway address. (Details not shown.)

Configuration files

Access switch ACCSW1

```
#
 sysname ACCSW1
#
 telnet server enable
#
 dhcp snooping enable
#
vlan 5
#
vlan 10
```

```
#
vlan 20
#
 stp bpdu-protection
#
interface Vlan-interface5
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
 dhcp snooping trust
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 5
#
line vty 0 63
 authentication-mode scheme
#
local-user admin class manage
 password hash
$h$6$ZJSf20ub4uEzjy2F$cXW3O3Jt5Ci21ECze7w2MdRpLebMaE4vXBo59frUrIZs+Knxw76oNBu+HiB0zqk
Tfrnw1Phe0rSRa5d+OSIIbg==
 service-type telnet
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

Access switches ACCSW2, ACCSW3, ACCSW4

The configuration files of access switches ACCSW2, ACCSW3, and ACCSW4 are the same as that of ACCSW1 except the VLAN IDs, management VLAN interface address, and interface numbers. (Details not shown.)

Core switch CORESW1

```
#
 sysname CORESW1
#
track 1 interface GigabitEthernet1/0/7
#
ospf 100 router-id 3.3.3.3
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
  network 172.16.3.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
 dhcp enable
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan 50
#
vlan 100
#
vlan 300
#
ftth
#
dhcp server ip-pool 1
 gateway-list 192.168.10.1
 network 192.168.10.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
 static-bind ip-address 192.168.10.254 mask 255.255.255.0 client-identifier aabb-cccc-dd
#
dhcp server ip-pool 2
 gateway-list 192.168.20.1
 network 192.168.20.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
#
```

```
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
interface Vlan-interface100
 ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.3.1 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.3.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5000
 vrrp vrid 1 track 1 priority reduced 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 300
#
```

Core switch CORESW2

The configuration file of core switch CORESW2 is the same as that of CORESW1 except the VLAN IDs, interface numbers, OSPF router ID, and VRRP group 1's priority. (Details not shown.)

Egress router

```
#
 sysname Router
#
 packet-filter default deny
#
 qos carl 1 source-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
 qos carl 2 source-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
 qos carl 3 destination-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
 qos carl 4 destination-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
```

```
#
ospf 10 router-id 1.1.1.1
 default-route-advertise always
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
  network 172.16.2.0 0.0.0.255
#
 dns proxy enable
 dns server 202.101.100.199
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 172.16.1.2 255.255.255.0
 packet-filter 2000 inbound
 qos car inbound carl 1 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car inbound carl 2 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 3 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 4 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
#
interface GigabitEthernet0/2
 port link-mode route
 ip address 172.16.2.2 255.255.255.0
 packet-filter 2000 inbound
 qos car inbound carl 1 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car inbound carl 2 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 3 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 4 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 202.101.100.2 255.255.255.252
#
 ip route-static 0.0.0.0 0 202.101.100.1
#
acl basic 2000
 rule 0 permit source 192.168.10.0 0.0.0.255
 rule 5 permit source 192.168.20.0 0.0.0.255
 rule 10 permit source 172.16.1.0 0.0.0.255
 rule 15 permit source 172.16.2.0 0.0.0.255
 rule 20 permit source 172.16.3.0 0.0.0.255
#
```

Related documentation

- Login management configuration in the fundamentals configuration guide for the device.
- Login management commands in the fundamentals command reference for the device.
- VLAN configuration in the Layer 2—LAN switching configuration guide for the device.
- VLAN commands in the Layer 2—LAN switching command reference for the device.

- Ethernet link aggregation configuration in the Layer 2—LAN switching configuration guide for the device.
- Ethernet link aggregation commands in the Layer 2—LAN switching command reference for the device.
- DHCP configuration in the Layer 3—IP services configuration guide for the device.
- DHCP commands in the Layer 3—IP services command reference for the device.
- OSPF configuration in the Layer 3—IP routing configuration guide for the device.
- OSPF commands in the Layer 3—IP routing command reference for the device.
- ACL configuration in the ACL and QoS configuration guide for the device.
- ACL commands in the ACL and QoS command reference for the device.
- QoS configuration in the ACL and QoS configuration guide for the device.
- QoS commands in the ACL and QoS command reference for the device.
- IP source guard configuration in the security configuration guide for the device.
- IP source guard commands in the security command reference for the device.