



# Ruijie RG-WLAN Series Access Points

## AP\_RGOS 11.9(6)W3B3

### Command Reference

Document Version: V1.0

Date: 2023.04.25

Copyright © 2023 Ruijie Networks

## Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark  and  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

## Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

# Preface

## Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

## Technical Support

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: [service\\_rj@ruijienetworks.com](mailto:service_rj@ruijienetworks.com)
- Live Chat: <https://www.ruijienetworks.com/rita>

## Conventions

### 1. Conversions

Convention	Description
<b>Bold font</b>	Commands, command options, and keywords are in <b>bold</b> font.
<i>Italic font</i>	Arguments for which you supply values are in <i>italic</i> font.
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

### 2. Signs

The signs used in this document are described as follows:

---

---

 **Warning**

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

---

---

 **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

---

---

 **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

---

---

 **Specification**

An alert that contains a description of product or version support.

---

**3. Note**

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

---





# Basic Configuration Commands

---

1. CLI Commands
2. Basic Management Commands
3. Line Commands
4. File System Commands
5. HTTP Commands
6. Syslog Commands
7. Software Upgrade Commands
8. Time Range Commands

# 1 CLI Commands

## 1.1 alias

Use this command to configure a command alias in global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**alias** *mode command-alias original-command*

**no alias** *mode command-alias*

**default alias** *mode [ command-alias ]*

### Parameter Description

Parameter	Description
<i>mode</i>	Mode of the command represented by the alias
<i>command-alias</i>	Command alias
<i>original-command</i>	Syntax of the command represented by the alias

### Defaults

Some commands in user or privileged EXEC mode have default alias.

### Command Mode

Global configuration mode

### Usage Guide

The following table lists the default alias of the commands in privileged EXEC mode.

Alias	Actual Command
h	help
p	ping
s	show
u	undebug
un	undebug

The default alias cannot be removed by the **no alias exec** command.

After configuring the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command.

The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use the **alias ?** command to list all the modes under which you can configure alias for commands.

```

Hostname(config)# alias ?
  aaa-gs          AAA server group mode
  acl             acl configure mode
  config         goble configure mode

```

The alias also has its help information that is displayed after \* in the following format:

```
*command-alias=original-command
```

For example, in the privileged EXEC mode, the default alias `s` stands for `show`. You can enter `s?` to query the key words beginning with `s` and the help information of the alias.

```
Hostname# s?
*s=show show start-chat start-terminal-service
```

If an alias represents more than one word, the command will be displayed in brackets. For example, if you set `sv` stand for `show version` in the privileged EXEC mode, then:

```
Hostname# s?
*s=show *sv="show version" show start-chat
start-terminal-service
```

The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias.

```
Hostname# s?
show start-chat start-terminal-service
```

The command alias also has its help information. For example, if the alias `ia` represents `ip address` in the interface configuration mode, then:

```
Hostname(config-if-GigabitEthernet 0/1)# ia ?
  A.B.C.D IP address
  dhcp    IP Address via DHCP
Hostname(config-if-GigabitEthernet 0/1)# ip address
```

The above help information lists the parameters of **ip address** and shows the actual command name.

You must enter an entire alias; otherwise it cannot be recognized.

Use the **show aliases** command to show the aliases setting in the system.

**Configuration Examples** The following example uses `def-route` to represent the default route setting of `ip route 0.0.0.0 0.0.0.0 192.168.1.1` in the global configuration mode:

```
Hostname# configure terminal
Hostname(config)# alias config def-route ip route 0.0.0.0 0.0.0.0
192.168.1.1
Hostname(config)# def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
Hostname(config)# end
Hostname# show aliases config
globe configure mode alias:
def-route          ip route 0.0.0.0 0.0.0.0
192.168.1.1
```

Related Commands	Command	Description
		<b>show aliases</b>

**Platform** N/A  
**Description**

## 1.2 privilege

Use this command to attribute the execution rights of a command to a command level in global configuration mode. Use the **no** form of this command to restore the default setting.

**privilege** *mode* [ **all** ] [ **level** *level* | **reset** ] *command-string*

**no privilege** *mode* [ **all** ] [ **level** *level* ] *command-string*

**Parameter Description**

Parameter	Description
<i>mode</i>	CLI mode of the command to which the execution rights are attributed.
<b>all</b>	Command alias
<b>level</b> <i>level</i>	Specifies the execution right levels (0–15) of a command or sub-commands
<b>reset</b>	Restores the command execution rights to its default level
<i>command-string:</i>	Command string to be authorized

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** The following table lists some key words that can be authorized by the **privilege** command in CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use the **privilege ?** command to list all CLI command modes that can be authorized.

Mode	Descripton
config	Global configuration mode.
exec	Privileged EXEC mode
interface	Interface configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
ip-dhcp-pool	DHCP address pool configuration mode
keychain	KeyChain configuration mode
keychain-key	KeyChain-key configuration mode

**Configuration Examples** The following example sets the password of CLI level 1 as **test** and attribute the **reload** rights to reset the device:

```
Hostname(config)# privilege exec level 1 reload
```

You can access the CLI window as level-1 user to usef the **reload** command:

```
Hostname> reload ?
```

```
LINE Reason for reload
```

<cr> You can use the key word **all** to attribute all sub-commands of reload to level-1 users:

```
Hostname(config)# privilege exec all level 1 reload
```

After the above setting, you can access the CLI window as level-1 user to use all sub commands of the **reload** command:

```

Hostname> reload ?
LINE      Reason for reload
at                reload at a specific time/date
cancel           cancel pending reload scheme
in              reload after a time interval
<cr>
    
```

<b>Related Commands</b>	Command	Description
	<b>enable secret</b>	Sets the CLI-level password.

**Platform** N/A.  
**Description**

### 1.3 show alias

Use this command to show all the command aliases or aliases in special command modes.

**show aliases** [ *mode* ]

<b>Parameter Description</b>	Parameter	Description
	<i>mode</i>	Mode of the command represented by the alias.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command displays the configuration of all aliases if no command mode is input.

**Configuration** The following example displays the command alias in privileged EXEC mode:

**Examples**

```

Hostname# show aliases exec
exec mode alias:
h                help
p                ping
s                show
u                undebug
un              undebug
    
```

<b>Related Commands</b>	Command	Description
	<b>alias</b>	Sets a command alias.

<b>Platform</b>	N/A.
<b>Description</b>	

# 1 Basic Management Commands

## 1.1 <1-99>

Use this command to restore the suspended Telnet Client session.

**<1-99>**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** This command is used to restore the suspended Telnet Client session. Hot keys (ctrl+shift+6 x) are used to exit the Telnet Client session creation. The **<1-99>** command is used to restore the session. If the session is created, you can use the **show session** command to display the session.

**Configuration** The following example restores the suspended Telnet Client session.

**Examples**

```
Hostname# 1
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 banner exec

Use this command to configure a message to welcome the user entering user EXEC mode through the line. Use the **no** form of this command to restore the default setting.

**banner exec c message c**

**no banner exec**

Parameter Description	Parameter	Description
	c	Separator of the message. Delimiters are not allowed in the message.

<i>message</i>	Contents of the message.
----------------	--------------------------

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol.  
 When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed.  
 The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the **no exec-banner** command on the line.

**Configuration Examples** The following example configures a welcome message.

```
Hostname(config)# banner exec $ Welcome $
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.3 banner incoming

Use this command to configure a prompt message for reverse Telnet session. Use the **no** form of this command to remove the setting.

**banner incoming** *c message c*  
**no banner incoming**

Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
<i>message</i>	Contents of the message.	

**Defaults** N/A

**Command Mode** Global configuration mode



**Usage Guide** This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol.

When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.

**Configuration** The following example configures a prompt message for reverse Telnet session.

**Examples**

```
Hostname(config)# banner incoming $ Welcome $
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.4 banner login

Use this command to configure a login banner. Use **no** form of this command to r remove the setting.

**banner login** *c message c*

**no banner login**

Parameter Description	Parameter	Description
	<i>c</i>	
	<i>message</i>	Contents of the login banner

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command sets the login banner message, which is displayed at login. The system discards all the characters next to the terminating symbol.

When a user logs in to the device, the MOTD information (configured using **banner motd**) and login banner information (configured using **banner login**) first appear. Upon login, the incoming prompt (**banner incoming**) is displayed in case of a reverse telnet connection and the EXEC prompt information (**banner exec**) is displayed in case of other connections.

**Configuration** The following example configures a login banner.

**Examples**

```
Hostname(config)# banner login $ enter your password $
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.5 banner motd

Use this command to set the Message-of-the-Day ( MOTD ) . Use the **no** form of this command to remove the setting.

**banner [ motd ] c message c**

**no banner [ motd ]**

**Parameter  
Description**

Parameter	Description
<i>c</i>	Separator of the MOTD. Delimiters are not allowed in the MOTD.
<i>message</i>	Contents of an MOTD

**Defaults**

N/A

**Command  
Mode**

Global configuration mode

**Usage Guide**

This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.

**Configuration** The following example configures the MOTD.

**Examples**

```
Hostname(config)# banner motd $ hello,world $
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.6 banner prompt-timeout

Use this command to configure the prompt-timeout message to notify timeout. Use the **no** form of this command to remove the setting.

**banner prompt-timeout** *c message c*

**no banner prompt-timeout**

### Parameter Description

Parameter	Description
<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
<i>message</i>	Contents of the message.

### Defaults

N/A

### Command Mode

Global configuration mode

### Usage Guide

The system discards all the characters next to the terminating symbol.  
When authentication times out, the banner prompt-timeout message is displayed.

### Configuration

The following example configures the prompt-timeout message to notify timeout.

### Examples

```
Hostname(config)# banner exec $ authentication timeout $
```

### Related Commands

Command	Description
N/A	N/A

### Platform

### Description

N/A

## 1.7 banner slip-ppp

Use this command to configure the slip-ppp message for the SLIP/PPP session. Use the **no** form of this command to remove the setting.

**banner slip-ppp** *c message c*

**no banner slip-pp**

### Parameter Description

Parameter	Description
<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
<i>message</i>	Contents of the message.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the slip-ppp message for the SLIP/PPP session. The system discards all the characters next to the terminating symbol.  
When the SLIP/PPP session is created, the slip-ppp message is displayed on the corresponding terminal.

**Configuration** The following example configures the banner slip-ppp message for the SLIP/PPP session.

**Examples**

```
Hostname(config)# banner slip-ppp $ Welcome to use this device. $
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.8 calendar set

Set the sysmte hardware time.

**calendar set** { *hour* [ :*minute* [ :*second* ] ] } [ *month* [ *day* [ *year* ] ] ]

**Parameter Description**


Parameter	Description
<i>hour</i> [ : <i>minute</i> [ : <i>second</i> ] ]	Sets hardware time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can be reset. The unspecified parameters keep the current system values.
<i>month</i>	Sets month. The range is from 1 to 12.
<i>day</i>	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
<i>year</i>	Sets year. The range is from 1970 to 2069.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value. For

example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **calendar set 12 5** command to change the current time into "2012-05-29 12:33:44".

 The hardware time of the system is used as the UTC time, while the software time of the system refers to the local time of the device.

 This command is supported only in VSD0 mode. Multiple VSDs are not supported.

**Configuration Examples** The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.


```
Hostname# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
Hostname# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Hostname# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

 Because the *hour* parameter is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.9 clock read-calendar

Configure the device to synchronize the software time based on the hardware time.

**clock read-calendar**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** After you configure this command, the system will synchronize the software time with the current hardware time according to the time zone and summer time settings of the device.

**Configuration** The following example enables the system to synchronize the software time with the hardware time.

**Examples**

```
Hostname# clock read-calendar
Set the system clock from the hardware time.
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.10 clock set

Configure the system date and clock.

**clock set** { *hour* [ *:minute* [ *:second* ] ] } [ *month* [ *day* [ *year* ] ] ]


**Parameter Description**

Parameter	Description
<i>hour</i> [ <i>:minute</i> [ <i>:second</i> ] ]	Sets software time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can reset. The unspecified parameters keep the current system values.
<i>month</i>	Sets month. The range is from 1 to 12.
<i>day</i>	Sets date. The range is from 1 to 31. If the day does not exist in the current month, the date is calculated backward.
<i>year</i>	Sets year. The range is from 1970 to 2069.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value.

 For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the **clock set 12 5** command to change the current time into "2012-05-29 12:33:44".

**Configuration Examples** The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters.


```
Hostname# clock set 6
06:48:13 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters.

```
Hostname# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.

```
Hostname# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

 Because the *hour* parameter in this command is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter **18** (hour), and then enter **3** (month) and **2** (day).

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.11 clock summer-time

Set the DST.

**clock summer-time** *zone* **start** *start-month* [*week*]**last** *start-date* *hh:mm* **end** *end-month* [*week*]**last** *end-date* *hh:mm* [**ahead** *hours-offset* [*minutes-offset* ]

Disable the DST.

**no clock summer-time**

**Parameter Description**

Parameter	Description
<b>zone</b>	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
<b>start</b>	Indicates the start time of the summer time.
<i>start-month</i>	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December.

	The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
<i>week</i>	Start week in the start month. The range is from 1 to 5.
<b>last</b>	The last week of the specified month.
<i>start-date</i>	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
<b>hh:mm</b>	Time, in the format of hour : minute.
<b>end</b>	Indicates the end time of the summer time.
<i>end-month</i>	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
<b>ahead</b>	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
<i>hours-offset</i>	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
<i>minutes-offset</i>	Minutes ahead of the standard time. The range is from 0 to 59. If <i>hours-offset</i> has been set to 0, you are not allowed to set <i>minutes-offset</i> to 0.

**Defaults** N/A

**Command Mode** configuration mode

**Usage Guide** N/A

**Configuration Examples** Assume that the time zone name of your living place is ABC and the standard time is 8:15 ahead of UTC, namely, GMT+08:15. The summer time period starts from the first Saturday in February to the third Monday in May and the summer time is 01:20 ahead of the standard time. In this case, the summer time is 09:35 ahead of the UTC time, but non-summer time is still 08:15 ahead of the UTC time.

```

Hostname(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
Hostname(config)#show clock
16:39:16 ABC Wed, Feb 29, 2012
Hostname(config)#show calendar
08:24:35 GMT Wed, Feb 29, 2012

Hostname(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead
1 20
    
```



```
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday
at 2:00 TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at
18:30, ahead 1 hour 20 minute

Hostname# show clock
18:00:08 TZA Wed, Feb 29, 2012

# If the time is set to non-summer time, the time zone name is restored to ABC.
Hostname#clo set 18 1 1
*Jan 1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan 1, 2012
Set system clock: 18:00:09 ABC Sun, Jan 1, 2012
Hostname#show clock
18:00:12 ABC Sun, Jan 1, 2012
```

If the system uses the default summer time that is one hour ahead of the standard time, ahead and the parameters behind ahead can be neglected. For example, set the summer time to start from 2:00 a.m. of the first Sunday in April to 2:00 a.m. of the last Sunday in October and set the summer time to one hour ahead of the standard time.

```
Hostname(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday
2:00
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at
2:00 TO October the last Sunday at 2:00, ahead 1 hour
Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at
2:00, ahead 1 hour
```

The following example disables summer time.

```
Hostname(config)#no clock summer-time
*Jan 1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

#### Related Commands

Command	Description
N/A	N/A

#### Platform Description

N/A


## 1.12 clock timezone

Use this command to set the time zone.

**clock timezone** [ *name* *hours-offset* [ *minutes-offset* ] ]

Use this command to remove the time zone settings.

**no clock timezone****Parameter  
Description**

Parameter	Description
<i>name</i>	Time zone name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The name contains 3 to 31 characters.
<i>hours-offset</i>	Hours of time difference. It indicates whether the time is faster or smaller than the hardware UTC time. The range is from -12 to 12. The negative digit indicates that the time is slower than the hardware time, while the positive digit indicates that the time is faster than the hardware time.   If the time is slower than the UTC time, add "-" before <i>hours-offset</i> .
<i>minutes-offset</i>	Minutes of time difference. The range is from 0 to 59.

**Defaults**

-

**Command  
Mode**

configuration mode

**Default Level**

-

**Usage Guide**

This command is supported only in VSD0 mode. Multiple VSDs are not supported.

**Configuration  
Examples**

The following example sets the time zone name to CST. The software time is 8 hours faster than the hardware time.

```

Hostname(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)

Hostname# show clock
18:00:17 CST Wed, Dec 5, 2012

```

The following example sets the time zone name TZA. The software time is 06:13 slower than the hardware time.

```

Hostname(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)

```

The following example removes the time zone settings.

```

Hostname(config)# no clock timezone
Set no clock timezone.

```

**Check Method**

-

**Platform**  
**Description** -

### 1.13 clock update-calendar

Use this command to enable the system to synchronize the hardware time with the software time.

**clock update-calendar**

**Parameter Description**

Parameter	Description
-	-

**Defaults** -

**Command Mode** Privileged EXEC mode

**Default Level** -

**Usage Guide** This command is supported only in VSD0 mode. Multiple VSDs are not supported. After you configure this command, the system will synchronize the hardware time with the current software time according to the time zone and summer time settings of the device.

**Configuration Examples** The following example enables the system to synchronize the hardware time with the software time.

```
Hostname# clock update-calendar
Set the hardware time from the system clock.
```

The following example sets the time zone of the hardware time to GMT+5:10, which indicates that the hardware time is 5:10 slower than the software time. The summer time is not set.

```
Hostname# show clock
09:30:21 TSZ Wed, Feb 29, 2012

Hostname# clock update-calendar
Set the hardware time from the system clock.
```

```
Hostname#show calendar
04:20:25 UTC Wed, Feb 29, 2012
```

The following example sets the hardware time. If it is set to GMT+5:10 and the summer time is set to be 1:15 faster from the first Monday in February 1 to the second Sunday in June 1, it indicates that the hardware time is 6:25 slower than the software time during the effective period of the summer time.

```
Hostname# show clock
```

```
09:30:02 TSZ Wed, Feb 29, 2012

Hostname# clock update-calendar
Set the hardware time from the system clock.

Hostname#show calendar
03:05:08 UTC Wed, Feb 29, 2012
```

**Check Method** -

**Platform**

**Description** -

## 1.14 configure

Use this command to enter global configuration mode.

**configure** [ **terminal** ]

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example enters global configuration mode.

**Examples**

```
Hostname# configure
Hostname(config)#
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.15 cpu high-watermark set

Use this command to set the high watermark of the CPU usage of the control core and enable CPU usage monitoring.

**cpu high-watermark set** [ [ **high** high-value ] [ **range** range-value ] ]

Use this command to disable CPU usage monitoring.

**no cpu high-watermark set**

Use this command to restore the default settings.

**default cpu high-watermark set**

Parameter Description	Parameter	Description
	<b>high</b> <i>high-value</i>	Sets the high watermark of the CPU usage. The range is from 2 to 99.
	<b>range</b> <i>range-value</i>	Sets the watermark fluctuation range. The range is from 1 to 20.
<b>Defaults</b>	By default, the watermark of the CPU usage is 80% and the watermark fluctuation range is 5% (namely, the range of the CPU usage watermark is from 75% and 85%).	
<b>Command Mode</b>	configuration mode	
<b>Default Level</b>	-	
<b>Usage Guide</b>	This command is supported only in VSD0 mode. Multiple VSDs are not supported. You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.	
<b>Configuration Examples</b>	<p>The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled).</p> <pre>Ruijie(config)# default cpu high-watermark set Reset default cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre> <p>The following example disables CPU usage monitoring.</p> <pre>Ruijie(config)# no cpu high-watermark set Close cpu watermark monitor</pre> <p>The following example enables CPU usage monitoring. Keep the defined watermark value.</p> <pre>Ruijie(config)# cpu high-watermark set Open cpu watermark monitor set system cpu watermark high 80%(75~85%)</pre>	

The following example enables CPU usage monitoring and sets the high watermark to 88% and fluctuation range to 3%.

```
Ruijie(config)# cpu high-watermark set high 88 range 3
Open cpu watermark monitor
set system cpu watermark high 88%(85%~91%)
```

In this case, the high watermark is set to 88%. The upper limit of the high watermark is 91% (88%+3%) and the lower limit is 85% (88%-3%).

**Check Method** -

**Prompt**

If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark:

**Message**

```
*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high watermark(85%), current cpu usage 100%
```

When the CPU usage is less than the lower limit of the high watermark, the system will print the following message about warning release:

```
*Jan 20 07:02:52: %RG_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%
```

**Platform**

-

**Description**

## 1.16 debug support

Enter the debug support mode  
**debug support**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command Mode**

Privileged EXEC mode

**Usage Guide**

This command is used to enter the debug support mode. You can run the Tech-Support commands only in debug support mode.

**Configuration Examples**

The following example enters the debug support mode.

```
Hostname# debug support
%Warning: Enter debug support mode, all commands in this mode are used to diagnose system hardware and software.

          Misuse of these commands will affect system performance. Therefore, use these commands under the guidance of Hostname Networks engineers.
```

<b>Related Commands</b>	Command	Description
	<b>enable</b>	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

**Platform Description** N/A

## 1.17 disable

Use this command to switch from privileged EXEC mode to user EXEC mode or lower the privilege level.


**disable** [ *privilege-level* ]

<b>Parameter Description</b>	Parameter	Description
	privilege-level	Privilege level

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** Use this command to switch to user EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.

 The privilege level that follows the **disable** command must be lower than the current level.

**Configuration Examples** The following example lowers the current privilege level of the device to level 10.

```
Hostname# disable 10
```

<b>Related Commands</b>	Command	Description
	<b>enable</b>	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.

**Platform Description** N/A

## 1.18 disconnect

Close a suspended telnet client session.

**disconnect** *session-id*

<b>Parameter Description</b>	Parameter	Description
	<i>session-id</i>	ID of the suspended telnet client session.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	You can run this command with a telnet client session ID specified to close the specified telnet client session.	
<b>Configuration Examples</b>	The following example closes telnet client session 1. Hostname# disconnect 1	
<b>Verification</b>	N/A	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.19 do telnet

Use this command to login to Telnet server.

**do telnet** *host* [ *port* ] [ /source { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* } ]

<b>Parameter Description</b>	Parameter	Description
	<i>host</i>	IPv4, IPv6 or host name of Telnet server.
	<i>port</i>	Configures TCP port ID. The default is 23.
	<b>/source</b>	Specifies source IP or source port for Telnet client.
	<b>ip</b> <i>A.B.C.D</i>	Specifies source IPv4 address for Telnet client.
	<b>ipv6</b> <i>X:X:X:X::X</i>	Specifies source IPv6 address for Telnet client.
	<b>interface</b> <i>interface-name</i>	Specifies source port for Telnet client.



<b>Defaults</b>	N/A
<b>Command Mode</b>	User EXEC mode/Privileged EXEC mode/Interface configuration mode
<b>Usage Guide</b>	N/A
<b>Configuration Examples</b>	<p>The following example configures destination IPv4 address 192.168.1.1, uses default port ID, and specifies source port Gi 0/1 and VRF table vpn1.</p> <pre>Ruijie(config)# do telnet 192.168.1.1 /source interface gigabitEthernet 0/1 /vrf vpn1</pre> <p>The following example configures destination IPv6 address 2AAA:BBBB::CCCC.</p> <pre>Ruijie(config)# do telnet 2AAA:BBBB::CCCC</pre> <p>The following example configures destination IPv4 address 192.168.1.1 and specifies MGMT port Mgmt 0.</p> <pre>Ruijie(config)# do telnet oob 192.168.1.1 via mgmt 0</pre>

<b>Related Commands</b>	Command	Description
	N/A	N/A

<b>Platform Description</b>	N/A
-----------------------------	-----

## 1.20 enable

Use this command to enter privileged EXEC mode.

**enable** [ *privilege-level* ]

<b>Parameter Description</b>	Parameter	Description
	<i>privilege-level</i>	Privilege level

<b>Defaults</b>	N/A
-----------------	-----

<b>Command Mode</b>	User EXEC mode
---------------------	----------------

<b>Usage Guide</b>	<p>This command is used to switch from the user EXEC mode to the privileged EXEC mode by default. If privilege level is specified, the current privilege level is raised to the specified level. When the RBAC function is enabled, this command can be used to switch the terminal role. If no role is specified, the system switches to role <b>network-admin</b> by default.</p>
--------------------	---

**Configuration** The following example lowers the privilege level to 14.

**Examples**

```
Hostname> enable 14
```

```
Password:
```

**Related Commands**

Command	Description
N/A	N/A

**Platform****Description**

N/A

## 1.21 enable password

Use this command to configure passwords for different privilege levels. Use the **no** form of this command to restore the default setting.

**enable password** [ *level level* ] [ { [ **0** ] [ *password* ] | **7 encrypted-password** } ]

**no enable password** [ *level level* ]

**Parameter Description**

Parameter	Description
<i>password</i>	Password for the user to enter the EXEC configuration layer
<b>level</b>	User's level.
<b>0</b>	The password is in plain text.
<b>7 encrypted-password</b>	The password is encrypted.

**Defaults**

N/A

**Command Mode**

Global configuration mode

**Usage Guide**

No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device.

A valid password is defined as follows:

- Consists of 1-26 upper/lower case letters and numbers
- Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the password.

If an encryption type is specified and a plaintext password is entered, you cannot enter privileged EXEC mode. A lost password that has been encrypted using any method cannot be restored. In this case, you can only reconfigure the device password.

**Configuration** The following example configures the password as pw10.

**Examples** Hostname(config)# enable password pw10

The following example configures the password as pw20 in interactive mode.

```
Hostname(config)# enable password
Please configure the password (1-126)
Enter Password:****
Confirm Password:****
```

**Related  
Commands**

Command	Description
<b>enable secret</b>	Sets the security password

**Platform  
Description**

N/A

## 1.22 enable secret

Use this command to configure a security password for different privilege levels. Use the **no** form of this command to restore the default setting.

**enable secret [ level *level* ] [ [ **0** ] [ *password* ] | { **5** | **8** } *encrypted-secret* ]**

**no enable secret [ level *level* ]**

**Parameter  
Description**

Parameter	Description
<b>level</b> <i>level</i>	User's level.
<b>0</b>	The password is in plain text.
<i>password</i>	Password for the user to enter the privileged EXEC configuration.
{ <b>5</b>   <b>8</b> } <i>encrypted- secret</i>	Configures the password encryption mode. <b>5</b> indicates that a password encrypted using the MD5 irreversible encryption algorithm is saved as an encrypted password. <b>8</b> indicates that a password encrypted using the SHA-256 irreversible encryption algorithm is saved as an encrypted password.

**Defaults**

N/A

**Command  
Mode**

Global configuration mode

**Usage Guide**

A password comes under two categories: "password" and "security". "Password" indicates a simple password, which can be set only for level 15. "Security" means a security password, which can be set for levels 0-15. If both types of passwords coexist in the system, no "password" type is allowed. If

a "password" type password is set for a level other than 15, the system gives an alert and the password is automatically converted into a "security" password. If a "password" type password is set for level 15 and the same as a "security" password, an alert is given. The password must be encrypted, with simple encryption for "password" type passwords and security encryption for "security" type passwords.

The cleartext password can be set in interactive mode.

**Configuration** The following example configures the security password as pw10.

**Examples**

```
Hostname(config)# enable secret 0 pw10
```

The following example configures the security password as pw20 in interactive mode.

```
Hostname(config)# enable secret
Please configure the password (1-126)
Enter Password:****
Confirm Password:****
```

**Related Commands**

Command	Description
<b>enable password</b>	Sets passwords for different privilege levels.

**Platform Description**

N/A

### 1.23 enable service

Use this command to enable or disable a specified service such as **SSH Server/Telnet Server/Web Server/SNMP Agent**.

**enable service { ssh-sesrver | telnet-server | web-server [ http | https | all ] | snmp-agent }**


**Parameter Description**

Parameter	Description
<b>ssh-server</b>	Enables SSH Server. IPv4 and IPv6 services are enabled at the same time.
<b>telnet-server</b>	Enables Telnet Server. IPv4 and IPv6 services are enabled at the same time.
<b>web-server [ http   https   all ]</b>	Enables HTTP Server. IPv4 and IPv6 services are enabled at the same time.
<b>snmp-agent</b>	Enables SNMP Agent. IPv4 and IPv6 services are enabled at the same time.

**Defaults** telnet-server, ssh-server, snmp-agent and web-server are disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable or disable a specified service. Use the **no enable service** command to disable the specified service.

 The **enable service web-server** command is followed by three optional keywords: [http | https | all]. If the command is followed by no keyword or by **all**, the command enables http and https services. Followed by **http**, the command enables http service only. Followed by **https**, the command enables https service only.

**Configuration** The following example enables the SSH server.

**Examples**

```
Hostname(Config)# enable service ssh-sesrver
```

**Related  
Commands**

Command	Description
<b>show service</b>	Displays the service status in the current system.

**Platform  
Description**

N/A

## 1.24 end

Use this command to return to privileged EXEC mode.

**end**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command  
Mode**

All modes except privileged EXEC mode

**Usage Guide**

N/A

**Configuration** The following example returns to privileged EXEC mode.

**Examples**

```
Hostname#con
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.25 exec-banner

Use this command to enable display of the EXEC message on a specific line. Use the **no** form of this command to restore the default setting.


**exec-banner**  
**no exec-banner**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** The EXEC message is displayed on all lines by default.

**Command Mode** LINE configuration mode

**Usage Guide** After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.

 This command does not work for the banner incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

**Configuration Examples** The following example disables display of the EXEC message on line VTY 1.

```
Hostname(config)# line vty 1
Hostname(config-line)no exec-banner
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.26 exec-timeout

Use this command to configure connection timeout for this device in LINE mode. Use the **no** form of this command to restore the default setting and the connection never expires.

**exec-timeout** *minutes* [ *seconds* ]

**no exec-timeout**

<b>Parameter Description</b>	Parameter	Description
	<i>minutes</i>	Timeout in minutes.
	<b>seconds</b>	(Optional) Timeout in minutes
<b>Defaults</b>	The default is 10 minutes.	
<b>Command Mode</b>	Line configuration mode	
<b>Usage Guide</b>	If there is no input or output for this connection within a specified time, this connection will expire, and this LINE will be restored to the free status.	
<b>Configuration Examples</b>	The following example sets the connection timeout to 5'30".	
	<pre>Hostname(config-line)#<b>exec-timeout</b> 5 30</pre>	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.27 execute

Use this command to execute a command on the file.

**execute** { [ **flash:** ] *filename* }

<b>Parameter Description</b>	Parameter	Description
	<i>filename</i>	Specifies the file path.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	

**Usage Guide** When the **execute** command is run, the device reads and executes character strings in the batch file line by line. When the file contains multiple commands, a line feed is required between different commands.

**Configuration** The following example executes a command to configure an IP address for the specified interface.

**Examples**

```

Hostname#execute flash:mybin/config.text
executing script file mybin/config.text .....
executing done
Hostname#config
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#ip address 192.168.21.158 24
Hostname(config-if-GigabitEthernet 0/1)#end
*Sep 29 23:35:49: %SYS-5-CONFIG_I: Configured from console by console

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.28 execute diagnose-cmd

Run the **execute diagnose-cmd** command to run the diagnose command.

**execute diagnose-cmd** { **help** | *shell-command* }

**Parameter Description**

Parameter	Description
<b>help</b>	Displays a list of executable <i>shell commands</i> .
<i>shell-command</i>	String of the shell command to be executed. For details about the command string, see <b>Usage Guide</b> . Whether this parameter is supported and its value range depend on the actual product.

**Defaults**

N/A

**Command Mode**

Debug support mode

**Usage Guide**

Command	Description
<b>at</b>	<b>at</b> diagnose command. For details about the parameter, see the device display.



<b>copy</b>	Copies files.
<b>delete</b>	Deletes files.
<b>df</b>	Displays the disk space usage.
<b>dir</b>	Displays the file list of the directory.
<b>dmesg</b>	Displays the core logs.
<b>du</b>	Displays the space usage of the file system.
<b>echo</b>	Saves data to a target file.
<b>fdisk</b>	Displays the partitioning information of a device.
<b>hexdump</b>	Displays the file information in hexadecimal format.
<b>kill</b>	Sends a signal to a specified process.
<b>md5sum</b>	Calculates and checks the MD5 message digest.
<b>mkdir</b>	Creates a directory.
<b>more</b>	Displays the file information.
<b>mount</b>	Displays the mounted file system.
<b>process</b>	Stops, starts, or restarts a process or a kernel module with the startup script.
<b>ps</b>	Displays information of the current process.
<b>redis-cli</b>	Database diagnose command
<b>rmdir</b>	Deletes an empty directory.
<b>sh</b>	Runs the module diagnose shell command.
<b>stat</b>	Displays the file or file system status.
<b>sync</b>	Updates the file system cache.
<b>tftp-tipc</b>	Transfers files through TFTP TIPC between different devices or cards.
<b>tipc-config</b>	Displays the TIPC neighbor node information.
<b>top</b>	Displays the process information.
<b>touch</b>	Creates an empty file or changes the timestamp of a file.

**Configuration** The following example displays the device configuration file.

**Examples**

```
Hostname(support)#execute diagnose-cmd more /data/config.text
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.29 exit

Use this command to return to the upper configuration mode.

**exit**

**Parameter  
Description**

Parameter	Description
-----------	-------------

N/A	N/A
-----	-----

**Defaults** N/A

**Command Mode** All configuration modes

**Usage Guide** N/A

**Configuration Examples** The following example returns to the upper configuration mode.

```

Hostname#con
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Hostname#con
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#line vty 0
Hostname(config-line)#exit
Hostname(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console
Hostname#exit

Press RETURN to get started

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.30 help

Use this command to display the help information.

**help**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

**Command** Any mode  
**Mode**

**Usage Guide** This command is used to display brief information about the help system. You can use "?" to display all commands or a specified command with its parameters.

**Configuration** The following example displays brief information about the help system.

**Examples**

```

Hostname#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.

2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

```

The following example displays all available commands in interface configuration mode.

```

Hostname(config-if-GigabitEthernet 0/1)#?
Interface configuration commands:
arp                ARP interface subcommands
bandwidth          Set bandwidth informational parameter
carrier-delay      Specify delay for interface transitions
dampening          Enable event dampening
default            Set a command to its defaults
description        Interface specific description
lldp               Exec data link detection command
duplex             Configure duplex operation
efm                Config efm for an interface
end                Exit from interface configuration mode
exit               Exit from interface configuration mode
expert             Expert extended ACL
flowcontrol        Set the flow-control value for an interface
full-duplex        Force full duplex operation
global             Global ACL
gvrp               GVRP configure command
half-duplex        Force half duplex operation
help               Description of the interactive help system
ip                 Interface Internet Protocol config commands
IPv6               Internet Protocol Version 6
l2                 Config L2 attribute
label-switching    Enable interface process mpls packet

```

lACP	LACP interface subcommands
lldp	Link Layer Discovery Protocol
load-interval	Specify interval for load calculation for an interface
mac	Mac extended ACL
mac-address	Set mac-address
mpls	Multi-Protocol Label Switching
mtu	Set the interface Maximum Transmission Unit (MTU)
no	Negate a command or set its defaults
ntp	Configure NTP
port-group	Aggregateport/port bundling configuration
redirect	Redirect packets
rmon	Rmon command
security	Configure the Security
show	Show running system information
shutdown	Shutdown the selected interface
snmp	Modify SNMP interface parameters
speed	Configure speed operation
vrrp	VRRP interface subcommands
xconnect	Xconnect commands

The following example displays the parameters of a specified command.

```

Hostname(config)#access-list 1 permit ?
A.B.C.D Source address
any Any source host
host A single source host

```

#### Related Commands

Command	Description
N/A	N/A

#### Platform Description

N/A

## 1.31 hostname

Use this command to specify or modify the hostname of a device.

**hostname** *name*

#### Parameter Description

Parameter	Description
<i>name</i>	Device hostname, string, number or hyphen, up to 63 characters.

#### Defaults

The default is Ruijie.

**Command** Global configuration mode  
**Mode**

**Usage Guide** This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.

**Configuration** The following example configures the hostname of the device as user\_Hostname.

**Examples**

```
Hostname(config)# hostname user_Hostname
user_Hostname (config)#
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.32 ip telnet source-interface

Use this command to configure the IP address of an interface as the source address for Telnet connection.

**ip telnet source-interface** *interface-name*

**Parameter  
Description**

Parameter	Description
<i>interface-name</i>	Configures the IP address of the interface as the source address for Telnet connection.

**Defaults** N/A

**Command  
Mode** Global configuration mode

**Usage Guide** This command is used to specify the IP address of an interface as the source address for global Telnet connection. When using the telnet command to log in a Telnet server, apply the global setting if no source interface or source address is specified. Use the **no ip telnet source-interface** command to restore it to the default setting.

**Configuration  
Examples** The following example configures the IP address of the *Loopback1* interface as the source address for global Telnet connection.

```
Hostname(Config)# ip telnet source-interface Loopback 1
```

Related Commands	Command	Description
		<b>telnet</b>

**Platform Description** N/A

## 1.33 lock

Use this command to set a temporary password for the terminal.

### lock

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** You can lock the terminal interface and maintain the session continuity to prevent access to the interface by setting a temporary password. Take the following steps to lock the terminal interface:

- Enter the **lock** command, and the system will prompt you for a password:
- Enter the password, which can be any character string. The system will prompt you to confirm the password, clear the screen, and display the "Locked" information.
- To access the terminal, enter the preset temporary password.
- To lock the terminal, run the **lockable** command in line configuration mode and enable terminal locking in the corresponding line.

**Configuration Examples** The following example locks a terminal interface.

#### Examples

```

Hostname(config-line)# lockable
Hostname(config-line)# end
Hostname# lock
Password: <password>
Again: <password>
Locked
Password: <password>
Hostname#

```

Related Commands	Command	Description
		<b>lockable</b>

**Platform**  
**Description**

N/A

## 1.34 lockable

Use this command to support the **lock** command at the terminal. Use the **no** form of this command to restore the default setting.

**lockable**  
**no lockable**

**Parameter**  
**Description**

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command** Line configuration mode  
**Mode**

**Usage Guide** This command is used to lock a terminal interface in the corresponding line. To lock the terminal, run the lock command in EXEC mode.

**Configuration** The following example enables terminal locking at the console port and locks the console.

**Examples**

```

Hostname(config)# line console 0
Hostname(config-line)# lockable
Hostname(config-line)# end
Hostname# lock
Password: <password>
Again: <password>
Locked
Password: <password>

```

**Related**  
**Commands**

Command	Description
<b>lock</b>	Locks the terminal.

**Platform**  
**Description**

N/A

## 1.35 login

Use this command to enable simple login password authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

**login**

**no login**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The login function is disabled for console and enabled for AUX, TTY, and VTY terminal by default.

**Command Mode** Line configuration mode

**Usage Guide** If the AAA security server is inactive, this command enables simple password authentication at login. The password is configured for a VTY or console interface.

**Configuration** The following example sets a login password authentication on VTY.

**Examples**

```

Hostname(config)# no aaa new-model
Hostname(config)# line vty 0
Hostname(config-line)# password 0 normatest
Hostname(config-line)# login

```

Related Commands	Command	Description
	<b>password</b>	Configures the line login password

**Platform Description** N/A

## 1.36 login access non-aaa

Use this command to configure non-AAA authentication on line when AAA is enabled.

**login access non-aaa**

Use the **no** form of this command to restore the default setting.

**no login access non-aaa**

Parameter Description	Parameter	Description
	N/A	N/A



**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** To perform non-AAA authentication for a line when AAA is enabled, run this command. The configuration is valid for all terminals.

**Configuration Examples** The following example configures local user authentication for virtual terminal 4 when AAA is enabled.

```

Hostname(config)#log access non-aaa
Hostname(config)#aaa new-model
Hostname(config)#line vty 0 4
Hostname(config-line)#login local
Hostname(config-line)#

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.37 login authentication

If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate AAA login authentication method list. Use the **no** form of this command to restore the default setting.

```

login authentication { default | list-name }
no login authentication { default | list-name }

```

**Parameter Description**

Parameter	Description
<b>default</b>	Name of the default authentication method list
<i>list-name</i>	Name of the method list

**Defaults** The default authentication method is used when AAA is enabled,

**Command Mode** Line configuration mode

**Usage Guide**

**Configuration** The following example associates the method list on VTY and perform login authentication on a radius server.

**Examples**

```

Hostname(config)# aaa new-model
Hostname(config)# aaa authentication login default radius
Hostname(config)# line vty 0
Hostname(config-line)# login authentication default

```

**Related Commands**

Command	Description
<b>aaa new-model</b>	Enables the AAA security service.
<b>aaa authentication login</b>	Configures the login authentication method list.

**Platform****Description**

N/A

## 1.38 login local

Use this command to enable local user authentication on the interface if AAA is disabled. Use the **no** form of this command to restore the default setting.

**login local****no login local****Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command Mode**

Line configuration mode

**Usage Guide**

If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the **username** command.

**Configuration** The following example sets local user authentication on VTY.

**Examples**

```

Hostname(config)# no aaa new-model
Hostname(config)# username test password 0 test
Hostname(config)# line vty 0
Hostname(config-line)# login local

```

**Related Commands**

Command	Description
<b>username</b>	Configures local user information.

**Platform**  
**Description**

N/A

## 1.39 login privilege log

Use this command to log privilege change.

**login privilege log**

Use the **no** form of this command to restore the default setting.

**no login privilege log**

**Parameter**  
**Description**

Parameter	Description
N/A	N/A

**Defaults** Enabled

**Command** Global configuration mode  
**Mode**

**Usage Guide** You can use this command to monitor privilege level increase or role switching of terminal users. The configuration is valid for all terminals.

**Configuration** The following example enables the logging function of privilege level increase.

**Examples** `Hostname(config)# login privilege log`

If the privilege level increase fails, the device prints the following log:

```
Hostname>enable 10
```

```
Password:
```

```
Password:
```

```
Password:
```

```
% Access denied
```

```
Hostname>
```

```
*Sep 10 11:34:19: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 10 from console failed
```

If the privilege level increase is successful, the device prints the following log:

```
Hostname>enable 10
```

```
Password:
```

```
Hostname#
```

```
*Sep 10 11:34:20: %SYS-5-PRIV_AUTH_SUCCESS: Authentication to privilege level 10 from console success
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.40 memory low-watermark set

Enable the monitoring of memory usage threshold.

**memory low-watermark set** *mem-rate*

Disable this feature.

**no memory low-watermark set**

Restore the default configuration.

**default memory low-watermark set**

**Parameter Description**

Parameter	Description
<i>mem-rate</i>	Memory usage threshold. The range is from 1% to 100%.

**Defaults**

The default memory usage threshold is **90%**.

**Command Mode**

Global configuration mode

**Usage Guide**

N/A

**Configuration Examples**

The following example sets the memory usage threshold to **80%** and enables the monitoring function of memory usage.

```
Hostname(config)#memory low-watermark set 80
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.41 memory history clear

Clear historical memory usage records.

**memory history clear [ one-forth | half | all ]**

Parameter Description	Parameter	Description
	<b>one-forth</b>	Clears 25% of historical information.
	<b>half</b>	Clears half of historical information.
	<b>all</b>	Clears all historical information.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears half of historical memory usage records.

```

Hostname# show memory history

Time Thu Jan  1 00:24:45 1970
Used(k) 148516
Maximum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      60600
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148492
Maximum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      52408
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148444
Maximum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      44088
rg_syslogd      36640

```

```

Hostname(config)#memory history clear half
2 out of 5 records in the history table to be cleared..
Clear done !

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.42 motd-banner

Use this command to enable display of the MOTD message on a specified line. Use the **no** form of this command to restore the default setting.

**motd-banner**  
**no motd-banner**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

The MOTD message is displayed on all lines by default.

**Command Mode**

Line configuration mode

**Usage Guide**

After you configure the **banner exec** and the **banner motd** commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the **no** form of this command on the line.



This command does not work for the incoming message. If you configure the **banner incoming** command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.

**Configuration**

The following example disables display of the MOTD message on VTY 1.

**Examples**

```

Hostname(config)# line vty 1
Hostname(config-line)no motd-banner

```

**Related Commands**

Command	Description
N/A	N/A

**Platform**  
**Description** N/A

## 1.43 password

Use this command to configure a password for line login, run the **password** command. Use the **no** form of this command to restore the default setting.

**password** [ { **0** [ *password* ] | **7** *encrypted-password* } ]

**no password**

**Parameter**  
**Description**

Parameter	Description
<i>password</i>	Password for remote line login
<b>0</b>	The password is in plain text.
<b>7</b> <i>encrypted-password</i>	The password is encrypted.

**Defaults** N/A

**Command**  
**Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example configures the line login password as **red**.

**Examples**

```
Hostname(config)# line vty 0
Hostname(config-line)# password red
```

The following example configures the line login password as **red** in interactive mode.

```
Hostname(config)# line vty 0
Hostname(config-line)# password
Please configure the password (1-25)
Enter Password:***
Confirm Password:***

Hostname(config-line)#
```

**Related**  
**Commands**

Command	Description
<b>login</b>	Moves from user EXEC mode to privileged EXEC mode or enables a higher level of authority.

**Platform**  
**Description** N/A

## 1.44 prompt

Use this command to set the **prompt** command. Use the **no** form of this command to restore the default setting.

**prompt string**

**no prompt**

### Parameter Description

Parameter	Description
<b>string</b>	Character string of the <b>prompt</b> command, containing up to 32 letters.

### Defaults

N/A

### Command Mode

Global configuration mode

### Usage Guide

If no prompt string is configured, the system name applies and varies with the system name. The **prompt** command is valid only in EXEC mode.

### Configuration Examples

The following example sets the prompt string to rgnos.

#### Examples

```

Hostname(config)# prompt rgnos
Hostname(config)# end
RGOS

```

### Related Commands

Command	Description
N/A	N/A

### Platform Description

N/A

## 1.45 reload

Restart the device immediately.

**reload [ at { hour [ :minute [ :second ] ] } [ month [ day [ year ] ] ] ]**

### Parameter Description

Parameter	Description
<i>hour [ :minute [ :second ] ]</i>	Scheduled restart time. hh indicates hours, mm indicates minutes, and ss indicates seconds.
<i>month</i>	Month. The range is from 1 to 12. If it is not specified, the current month of the system is used.



<i>day</i>	Day. The range is from 1 to 31. If a day does not exist in a month, the day is moved to the following day. If it is not specified, the current day of the system is used.
<i>year</i>	Year. The range is from 1970 to 2069. If it is not specified, the current year of the system is used.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example restarts the device.

**Examples** Hostname# reload

```
Reload system?(Y/N) Y
Sending all processes the TERM signal... [ OK ]
Sending all processes the KILL signal... [ OK ]
Restarting system...
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.46 secret

Use this command to set a password encrypted by irreversible MD5/SHA256 for line login. Use the no form of this command to restore the default setting.

**secret** { [ 0 ] *password* | { 5 | 8 } *encrypted-secret* }  
**no secret**

**Parameter Description**

Parameter	Description
<b>0</b>	(Optional) sets the plaintext password text and encrypts it with irreversible MD5 after configuration.
<i>password</i>	Sets the password plaintext, a string ranging from 1 to 25 characters.
{ 5   8 } <i>encrypted-secret</i>	5 specifies a password encrypted using the MD5 irreversible encryption algorithm. The password is saved as an encrypted password after configuration. 8 specifies a password encrypted using


	the SHA-256 irreversible encryption algorithm. The password is saved as an encrypted password after configuration.
--	--


**Defaults** N/A


**Command mode** Line configuration mode


**Usage Guide** This command is used to set a password encrypted by irreversible MD5 that is authenticated by a remote user through line login.

The cleartext password can be configured in interactive mode.

 If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the first, third, and eighth characters of the password text must be \$.

 If the value **8** is selected for the encryption type, the entered ciphertext password must contain 56 characters with the 1st, 4th, and 15th, and 56th characters set to the dollar sign (\$).

 In general, the encryption type does not need to be specified as 5 or 8 except when the encrypted password is copied and pasted.

 Line mode allows configuration of both “password” and “secret” types passwords at the same time. When the two passwords are the same, the system will send alert notification but the configuration will be permitted. When the system is configured with the two passwords, if the user enters a password that does not match the “secret” type password, it will not continue to match the “password” type password and login fails, enhancing security for the system password.

**Configuration** The following example sets the password encrypted by irreversible MD5 for line login to vty0.

**Examples**

```

Hostname(config)# line vty 0
Hostname(config-line)# algorithm-type md5
Hostname(config-line)# secret vty0

```

The following displays the encryption outcome by running the **show** command.

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

The following example configures the line login password as vty1 in interactive mode.

```

Hostname(config)# line vty 0
Hostname(config-line)# secret

Please configure the password (1-25)

Enter Password:****
Confirm Password:****

```

```
Hostname(config-line)#
```

**Related Commands**

Command	Description
<b>login</b>	Sets simple password authentication on the

	interface as the login authentication mode
--	--

**Platform** N/A  
**Description**

### 1.47 session-timeout

Use this command to configure the session timeout for a remote terminal. Use the **no** form of this command to restore the default setting and the session never expires.

**session-timeout** *minutes* [ **output** ]  
**no session-timeout**

Parameter Description	Parameter	Description
		<i>minutes</i>
	<b>output</b>	Regards data output as the input to determine whether the session expires.

**Defaults** The default timeout is 0.

**Command Mode** LINE configuration mode

**Usage Guide** If no input or output in current LINE mode is found on the remote terminal for the session within a specified time, this connection will expire, and this LINE will be restored to the free status.

**Configuration** The following example specifies the timeout as 5 minutes.

**Examples** `Hostname(config-line)#session-timeout 5 output`

Related Commands	Command	Description
		N/A

**Platform** N/A  
**Description**

### 1.48 show calendar

Display the hardware time of the system.

**show calendar**

Parameter Description	Parameter	Description

	N/A	N/A				
<b>Defaults</b>	N/A					
<b>Command Mode</b>	All modes except the user EXEC mode					
<b>Usage Guide</b>	N/A					
<b>Configuration Examples</b>	The following example displays the hardware time of the system.					
	<pre> Hostname# show calendar 21:57:48 GMT Sun, Feb 28, 2012 </pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
<b>Platform Description</b>	N/A					

## 1.49 show clock

Display the software time of the system.

**show clock**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A	
Parameter	Description					
N/A	N/A					
<b>Defaults</b>	N/A					
<b>Command Mode</b>	All modes except the user EXEC mode					
<b>Usage Guide</b>	N/A					
<b>Configuration Examples</b>	The following example displays the software time of the system.					
	<pre> Hostname&gt; enable Hostname# show clock 18:22:20 UTC Thu, May 20, 2021 </pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> </tbody> </table>	Command	Description			
Command	Description					

N/A	N/A
-----	-----

**Platform**  
**Description**

N/A

## 1.50 show cpu

Display CPU usage information of system tasks on control cores and non-virtual cores.

**show cpu**

**Parameter**  
**Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command**  
**Mode**

All modes except the user EXEC mode

**Usage Guide** This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid. If the system is equipped with a virtual core, you can run the **show processes cpu** command to display the CPU usage of the virtual core.

**Configuration** The following example displays CPU usage of system tasks on control cores and non-virtual cores.

**Examples**

```

Hostname#show cpu
=====
CPU Using Rate Information
CPU utilization in five seconds: 4.80%
CPU utilization in one minute: 4.10%
CPU utilization in five minutes: 4.00%

NO      5Sec   1Min   5Min Process
  1  0.00%  0.00%  0.00% init
  2  0.00%  0.00%  0.00% kthreadd
  3  0.00%  0.00%  0.00% ksoftirqd/0
  4  0.00%  0.00%  0.00% events/0
--More--

```

**Related**  
**Commands**

Command	Description
N/A	N/A

**Platform**  
**Description** N/A

## 1.51 show debugging

Check whether the debugging function of the device is enabled.

**show debugging**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example checks whether the debugging function of the device is enabled.

```

Hostname#show debugging

debug fw-group detect intf-state

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.52 show hostname

Display the host name of the device.

**show hostname**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the host name of the device. The following example displays the host name of the device.

```

Hostname#show hostname
Hostname
Hostname#

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.53 show line

Use this command to display the configuration of a line.

**show line** { **console** *line-num* | **vty** *line-num* | *line-num* }

**Parameter Description**

Parameter	Description
<b>console</b>	Display s the configuration of a console line.
<b>vty</b>	Display s the configuration of a vty line.
<i>line-num</i>	Number of the line.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

**Configuration Examples** The following example displays the configuration of a console port.

```

Hostname# show line console 0
CON      Type      speed  Overruns
* 0      CON      9600   45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation

```

```

      ^x   none   ^M
Timeouts:   Idle EXEC   Idle Session
            never     never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output: 395756 bytes
Data overflow: 27697 bytes
stop rx interrupt: 0 times
    
```

Field	Description
CON	Terminal type. <b>CON</b> indicates the console. <b>0</b> indicates the terminal line ID. The ID with an asterisk (*) indicates the terminal line that is being used.
Type	Terminal type, including <b>CON</b> , <b>AUX</b> , <b>TTY</b> , and <b>VTY</b> .
speed	Asynchronous speed
Overruns	Count of overrun errors received by the driver
Line 0	Terminal line ID
Location: ""	Line location
Type: "vt100"	Compatible terminal standard of a line
Special Chars	Special characters of a terminal, including the <b>Escape</b> , <b>Disconnect</b> , and <b>Activation</b> characters
Timeouts	Timeout time of a terminal session. <b>never</b> indicates that a session never times out.
History	Historical command recording function and the maximum number of recorded historical commands.
Total input	Count of data received from the driver
Total output	Count of data sent to the driver
Data overflow	Count of received data that overflows
stop rx interrupt	Count of RX interrupts of the driver

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.54 show memory

Display memory information.

**show memory** [ **sorted total** | **history** | **low-watermark** | *process-id* | *process-name* ]



Parameter Description	Parameter	Description
	<b>sorted total</b>	Sorts tasks based on the memory usage.
	<b>history</b>	Displays historical memory usage records.
	<b>low-watermark</b>	Displays the memory usage lower threshold.
	<i>process-id</i>	Task ID. The value ranges from 0 to 32768.
	<i>process-name</i>	Task name.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** Each time the **show memory history** command is run, the number of displayed entries increases by one. Up to 10 entries are displayed. You can run the **memory history clear** command to clear historical entries.

**Configuration Examples** The following example displays the memory usage of each task and its ranking by total memory usage.

```

Hostname# show memory sorted
System Memory: 508324K total, 481560K used, 26764K free, 348200K available, 50.5% used
rate
Swap:          128000K total, 128000K free
Used detail:   149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others

PID   Text (K)  Rss (K)  Data (K)      Stack (K)  Total (K)  Process
807   1568     4584    264728        84         270028    tcpip.elf
854    40       1436    246076        84         248840    cli-filesystem
1237  52       1492    123260        84         126036    cli-memory
803   56       1104    74064         84         76920     ping.elf
727   84       1276    33812         84         36640     rg_syslogd
733   84       796    33536         84         36364     rg_syslogd
776  224     1416    16896         84         19800     lsmdemo
858   40      1324    16844         84         19612     rg-tty-admin
769   40      3600    11052         84         13812     skbdemo
--More--
    
```

Field	Description
total	Total memory size of the system
used	Size of the used memory
free	Size of the remaining memory
available	Size of the remaining available memory, including the idle memory size and idle swap area size

used rate	Memory usage in percentage For devices that use a swap area, the memory usage includes the swap area usage.
Swap	Total size and idle size of the swap area
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by the slab
others	Size of the used memory excluding the memory occupied by active and inactive pages, mapped memory, and slab memory.

Field	Description
PID	Process ID
Text	Code segment size
Rss	Resident memory size
Data	Data segment size
Stack	Stack size
Total	Total used memory
Process	Task name

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.55 show memory vsd

Display memory information.

**show memory vsd** *vsd\_id*

**Parameter Description**

Parameter	Description
<i>vsd_id</i>	ID of the specified VSD. The range is from 0 to 16.

**Defaults**

N/A

**Command Mode**

All modes except the user EXEC mode

**Usage Guide**

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

**Configuration** The following example displays the memory usage of tasks under VSD 1.

**Examples**

```

Hostname#show memory vsd 1
PID      Text    Rss     Data   Stack  Total  Process
1408     244     1192    25400  84     32164  tty_secu_enable
1385     104     16288   648    84     18648  gvpd
1384     304     3872    17084  84     24728  wbamain
1382     376     17708   33656  84     53308  snooping.elf
1381     84      2156    16736  84     22956  password_policy
1380     72      1096    404    84     3848   dns_client.elf
1379     168     2580    472    84     5352   rg-rmond
1378     652     3504    9768   84     15964  rg-snmpd
1376     208     1452    10672  84     14872  rg-fsui
1375     116     2020    33464  84     37288  rg-telnetc
1373     24      844     220    84     2824   rg-telnetd
1372     724     2364    17016  84     24380  rg-sshd
1371     244     2996    35780  84     42544  rg-tty-admin
1365     132     2168    9004   84     13796  vrrp_plus.elf
1364     312     16944   764    84     20368  vrrp.elf
1363     124     16988   500    84     19744  lacp.elf
1358     24      1380    320    84     3536   ftpc_cli.elf
1357     124     1944    8552   84     14976  ftp_server.elf
1352     340     3032    74704  84     80768  dhcp6.elf
1351     312     1960    988    84     6116   dhcp.elf
1350     388     17808   920    84     21600  mstp.elf
1349     240     3876    976    84     9536   rpi.elf
1347     212     4220    872    84     9368   ripng.elf
1345     460     4284    876    84     9656   rip.elf
1340     1084    4700    1024   84     10928  ldap.elf
1339     288     17684   556    84     21472  msf.elf
1338     208     3604    42712  84     47708  rg-syslogd
--More--

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.56 show pci-bus

Display information about devices mounted on the Peripheral Component Interconnect (PCI) bus.

**show pci-bus**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide**

**Configuration** The following example displays information about devices mounted on the PCI bus.

**Examples**

```

Hostname# show pci-bus
NO:0
Vendor ID           : 0x1131
Device ID           : 0x1561
Domain:bus:dev.func : 0000:00:05.0
Status / Command    : 0x2100000
Class / Revision    : 0xc031030
Latency             : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a

NO:1
Vendor ID           : 0x1131
Device ID           : 0x1562
Domain:bus:dev.func : 0000:00:05.1
Status / Command    : 0x2100156
Class / Revision    : 0xc032030
Latency             : 0x30
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.57 show processes cpu

Display system tasks.

**show processes cpu** [ **history** [ **table** ] ] [ **5sec** | **1min** | **5min** | **15min** ] [ **nonzero** ] [ **record** ]

Parameter Description	Parameter	Description
	<b>5sec</b>	Displays tasks in descending order of the CPU usage within the last 5 seconds.
	<b>1min</b>	Displays tasks in descending order of the CPU usage within the last 1 minute.
	<b>5min</b>	Displays tasks in descending order of the CPU usage within the last 5 minutes.
	<b>15min</b>	Displays tasks in descending order of the CPU usage within the last 15 minutes.
	<b>nonzero</b>	Not displays information about the tasks whose CPU usage is 0.
	<b>history</b>	Displays the CPU usage of control core tasks within the last 60 seconds, 60 minutes, and 72 hours in histogram.
	<b>table</b>	Displays the CPU usage of control core tasks within the last 60 seconds, 60 minutes, and 72 hours in table.
	<b>record</b>	Displays the CPU usage of control core tasks within 5 minutes and the top 5 tasks in the CPU usage within 5 minutes.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

**Configuration Examples** The following example displays tasks in ascending order of their IDs.

```

Hostname# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)

Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S  PRI  P    5Sec    1Min    5Min    15Min Process
   1  0 S   20  0   0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) init
   2  0 S   20  1   0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) kthreadd
    
```

```

3  0 S  -100  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/0
4  0 S   20  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) ksoftirqd/0
5  0 S  -100  1  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/1

--More--
    
```

The following example displays tasks in ascending order of task ID. The tasks whose CPU usage is 0 within 15 minutes are not displayed.

```

Hostname# show processes cpu nonzero
    
```

Field	Description
System Uptime	Total running time of the device, accurate to seconds
CPU Utilization	Total CPU usage of control core tasks within the last 5 seconds, 1 minute, and 5 minutes
Virtual CPU usage	Total CPU usage of virtual core tasks within the last 5 seconds, 1 minute, and 5 minutes
Tasks Statistics	Task statistics, including the total number of tasks and the task status
set system cpu watermark	CPU usage threshold and status of the control core tasks

Task Running Status	Description
running	Running task
sleeping	Suspended task
stopped	Stopped task
zombie	Terminated task, but not reclaimed by the system

Field	Description
Pid	Task ID
Vsd	VSD ID
S	Task statuses, including <b>R</b> (running), <b>T</b> (stopped), <b>S</b> (sleeping), <b>D</b> (waiting), and <b>Z</b> (zombie)
PRI	Task priority
P	CPU core on which a task runs
5sec/1min/5min/15min	CPU usage of a task within the last 5 seconds, 1 minute, 5 minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores of the same type as the core where the task runs.
Process	Task name. Only the first 15 characters are displayed. The remaining characters are truncated.

The following example displays threads with non-zero CPU usage within 15 minutes only, in ascending order of task ID.

```

Hostname #show processes cpu nonzero
    
```







```

#-----#
|          | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
#-----#
#-----#
|          | 0 | 2.0 | 2.4 | 2.3 | 2.3 | 2.8 | 3.0 | 2.7 | 3.2 | 2.6 | 2.4 |
#-----#
|          | 1 | 2.7 | 2.5 | 2.7 | 2.2 | 2.4 | 2.6 | 2.2 | 2.7 | 2.3 | 2.5 |
#-----#
|          | 2 | 2.9 | 2.0 | 2.4 | 2.5 | 2.7 | 2.4 | 2.4 | 2.6 | 2.6 | 2.5 |
#-----#
|          | 3 | 2.7 | 2.8 | 2.8 | 3.2 | 2.5 | 3.2 | 3.1 | 4.0 | 2.7 | 2.7 |
#-----#
|          | 4 | 4.0 | 2.3 | 2.1 | 2.2 | 2.7 | 2.4 | 2.5 | 2.6 | 2.4 | 2.6 |
#-----#
|          | 5 | 2.4 | 3.2 | 2.5 | 2.3 | 2.3 | 3.6 | 2.8 | 2.5 | 2.2 | 2.4 |
#-----#

          system cpu percent usage (%) [last 60 minute]
#-----#
|          | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
#-----#
#-----#
|          | 0 | 2.6 | 2.5 | 3.0 | 2.4 | 2.6 |
#-----#

```

The following example displays the CPU usage of control core tasks every 5 minutes in the last week that exceeds the CPU usage threshold.

```

Hostname#show processes cpu record
CPU watermark high up 9%, down 6%

1970-01-07 01:20:13    system(11.0%)  ssa_process(9.1%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  rl-con/0(0.2%)
1970-01-07 01:25:26    system(10.8%)  ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  lsm.elf(0.2%)
1970-01-07 01:30:39    system(10.5%)  ssa_process(9.0%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  rg-sysmon(0.2%)
1970-01-07 01:35:52    system(10.5%)  ssa_process(9.0%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.2%)
1970-01-07 01:41:05    system(10.7%)  ssa_process(9.1%)  ssd_process(0.6%)
ssc_process(0.3%)  ham(0.3%)  lsm.elf(0.2%)
1970-01-07 01:46:18    system(10.7%)  ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.2%)
1970-01-07 01:51:31    system(10.8%)  ssa_process(9.1%)  ssd_process(0.6%)  rg-
sysmon(0.3%)  ssc_process(0.3%)  ham(0.3%)

```

```

1970-01-07 01:56:45      system(10.9%)  ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.3%)
1970-01-07 02:01:58      system(11.0%)  ssa_process(9.1%)  ssd_process(0.7%)  rg-
sysmon(0.4%)  ssc_process(0.3%)  ham(0.3%)
1970-01-07 02:07:11      system(11.0%)  ssa_process(9.1%)  ssd_process(0.7%)  rg-
sysmon(0.4%)  ham(0.3%)  ssc_process(0.3%)
1970-01-07 02:12:24      system(11.0%)  ssa_process(9.1%)  ssd_process(0.7%)  rg-
sysmon(0.4%)  ssc_process(0.3%)  ham(0.3%)
1970-01-07 02:17:37      system(11.0%)  ssa_process(9.0%)  ssd_process(0.6%)  rg-
sysmon(0.4%)  ham(0.3%)  ssc_process(0.3%)
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.58 show processes cpu detailed

Display details about a specific task.

**show processes cpu detailed** { *process-id* | *process-name* }

**Parameter Description**

Parameter	Description
<i>process-id</i>	ID of a specified task.
<i>process-name</i>	Name of a specified task.

**Defaults**

N/A

**Command Mode**

All modes except the user EXEC mode

**Usage Guide**

This command is supported by VSD 0 only. In multi-VSD mode, this command is invalid.

**Configuration**

The following example displays details about a task with the specified name.

**Examples**

```

Hostname# show processes cpu detailed demo
Process Id      : 1820
Process Name    : demo
Vsdid          : 0
Process Ppid    : 1

State          : R(running)
On CPU         : 0
    
```

```

Priority      : 20
Age Time     : 24:06.5
Run Time     : 00:01.0
Cpu Usage    :
  Last 5 sec  0.3% (0.6%)
  Last 1 min  0.3% (0.6%)
  Last 5 min  0.3% (0.6%)
  Last 15 min 0.3% (0.6%)
Tty          : ?
Code Usage   : 209.6KB.

```

If the specified task name is not unique, the system displays the following information:

```

Hostname# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
name: demo, id: 1091, state: R(running)
process name: monitor_procs, do NOT exist, or NOT only one.

```

Field	Description
Process Id	Task ID
Vsdid	ID of the VSD to which the task belongs
Process Name	Task name
Process Ppid	Parent process task ID
State	Task running status
On CPU	CPU where the task is running
Priority	Task priority
Age Time	Duration of the task from startup to now
Run Time	Execution duration of the task from startup to now
Cpu Usage	<p><b>CPU usage of the task within the last 5 seconds, 1 minute, 5 minutes, and 15 minutes</b></p> <p>The value in the round brackets is the CPU usage that is not divided by the total number of cores of the same type as the core where the task runs. For example, the demo task is running on core 0, which is a control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%).</p>
Tty	TTY ID, in the format of "Master device ID, slave device ID". If the TTY ID is <b>0</b> , a question mark (?) is displayed.
Code Usage	Size occupied by the task code segment

The following example displays details about a task with the specified ID.

```

Hostname# show process cpu detailed 1715
Process Id   : 130
Process Name : crypto
Vsdid       : 0
Process Ppid : 2

```

```

State       : S(sleeping)
On CPU     : 0
Priority    : 0
Age Time   : 03:41:09.9
Run Time   : 00:00.0
Cpu Usage  :
  Last 5 sec  0.0%( 0.0%)
  Last 1 min  0.0%( 0.0%)
  Last 5 min  0.0%( 0.0%)
  Last 15 min 0.0%( 0.0%)
Tty        : ?
Code Usage  : 0.0KB.

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.59 show reboot-reason

Display the device restart reasons.

**show reboot-reason [ all ]**

**Parameter  
Description**

Parameter	Description
<b>all</b>	Displays restart reasons of all devices.

**Defaults**

N/A

**Command  
Mode**

All modes except the user EXEC mode

**Usage Guide**
**Configuration**

The following example displays the device restart reasons.

**Examples**

```

Hostname#show reboot-reason
time: 1970-01-01 08:03:13
reason: reload cmd
info: /sbin/rg-sysmon/3844

Hostname#

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.60 show reload

Use this command to display the system restart settings.

**show reload**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

### Usage Guide

**Configuration** The following example displays the restart settings of the system.

**Examples**

```

Hostname# show reload
Reload scheduled in 595 seconds.
At 2003-12-29 11:37:42
Reload reason: test.

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.61 show running-config

Use this command to display how the current device system is configured.

**show running-config [ interface *interface* ]**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	N/A	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.62 show service

Use this command to display the service status.

**show service**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example displays whether the service is enabled or disabled.	
	<pre> Hostname# show service web-server      : disabled web-server(https): disabled snmp-agent      : enabled ssh-server      : enabled </pre>	

```
telnet-server : disabled
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.63 show sessions

Use this command to display the Telnet Client session information.

**show sessions****Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command  
Mode**

User EXEC mode

**Usage Guide**

Telnet Client session information includes the VTY number and the server IP address.

**Configuration**

The following example displays the Telnet Client session information.

**Examples**

```
Hostname#show sessions
Conn  Address
*1    127.0.0.1
*2    192.168.21.122
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.64 show startup-config

Use this command to display the device configuration stored in the Non Volatile Random Access Memory (NVRAM).

**show startup-config**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	<p>The device configuration stored in the NVRAM is executed while the device is starting.</p> <p>On a device that does not support <b>boot config</b>, <b>startup-config</b> is contained in the default configuration file <b>/config.text</b> in the built-in flash memory.</p> <p>On a device that supports <b>boot config</b>, configure <b>startup-config</b> as follows:</p> <p>If you have specified a boot configuration file using the <b>boot config</b> command and the file exists, <b>startup-config</b> is stored in the specified configuration file.</p> <p>If the boot configuration file you have specified using the <b>boot config</b> command does not exist or you have not specified a boot configuration file using the command, <b>startup-config</b> is contained in <b>/config.text</b> in the built-in flash memory.</p>	
<b>Configuration Examples</b>	N/A	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>boot config</b>	Sets the name of the boot configuration file.
<b>Platform Description</b>	N/A	

## 1.65 show usb-bus

Display information about devices mounted on the USB bus.

**show usb-bus**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	All modes except the user EXEC mode	



**Usage Guide** N/A

**Configuration** The following example displays information about devices mounted on the USB bus.

**Examples**

```
Hostname# show usb-bus
Device: Linux Foundation 2.0 root hub
  Bus 001 Device 001: ID 1d6b:0002
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

**Description**

N/A

## 1.66 show version

Display the system version.

**show version**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command  
Mode**

All modes except the user EXEC mode

**Usage Guide**

N/A

**Configuration** The following example displays the system version.

**Examples**

```
Hostname# show version
System description      : Hostname Indoor AP320-I (802.11a/n and 802.11b/g/n) By Hostname
Networks
System start time      : 2012-12-06 00:00:00
System uptime          : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number   : 1234942570018
System boot version    : 1.0.0
```

**Related  
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

**Platform**  
**Description**

N/A

## 1.67 speed

Use this command to set the speed at which the terminal transmits packets. Use the **no** form of this command to restore the default setting.

**speed** *speed*

**no speed**

**Parameter**  
**Description**

Parameter	Description
<i>speed</i>	Transmission rate (bps) on the terminal. For serial ports, optional rates include 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.

**Defaults** The default is 9600.

**Command** Line configuration mode  
**Mode**

**Usage Guide** This command is used to set the speed at which the terminal transmits packets.

**Configuration** The following example sets the rate of the serial port to 57600 bps.

**Examples**

```
Hostname(config)# line console 0
Hostname(config-line)# speed 57600
```

**Related**  
**Commands**

Command	Description
N/A	N/A

**Platform**  
**Description**

N/A

## 1.68 telnet

Use this command to log in a server that supports telnet connection.

**telnet** *host* [ *port* ] [ /**source** { **ip** *A.B.C.D* | **IPv6** *X:X:X:X::X* | **interface** *interface-name* } ]

**Parameter**  
**Description**

Parameter	Description
-----------	-------------

<i>host</i>	The IP address of the host or host name you want to log in.
<i>port</i>	Selects the TCP port number for login, 23 by default.
<i>/source</i>	Specifies the source IP address or source interface used by the Telnet client.
<b>ip</b> A.B.C.D	Specifies the source IPv4 address used by the Telnet client.
<b>IPv6</b> X:X:X:X::X	Specifies the source IPv6 address used by the Telnet client.
<b>interface</b> <i>interface-name</i>	Specifies the source interface used by the Telnet client.

**Defaults** N/A

**Command Mode** User EXEC mode

**Usage Guide** This command is used to log in a telnet server.

The **/vrf** keyword only applies to the RSR series of routers.

The **/ipv6** keyword only applies to IPv6-supported devices, such as S3760, S57 and S86.

**Configuration Examples** The following example sets the IPv6 address of the telnet server to **2AAA:BBBB::CCCC**.

```
Hostname# telnet 2AAA:BBBB::CCCC
```

The following example sets the IPv4 address of the telnet server to **192.168.1.1**.

```
Hostname# telnet 192.168.1.1
```

**Related Commands**

Command	Description
<b>ip telnet source-interface</b>	Specifies the IP address of the interface as the source address for Telnet connection.
<b>show sessions</b>	Displays the currently established Telnet sessions.
<b>exit</b>	Exits current connection.

**Platform Description** N/A

## 1.69 username

Use this command to set a local username and optional authorization information. Use the **no** form of this command to restore the default setting.

```
username name [ login mode { console | ssh | telnet } ] [ online amount number ] [ permission oper-mode path ] [ privilege privilege-level ] [ reject remote-login ] [ web-auth ] [ pwd-modify ] [ nopassword | password [ [ 0 | 7 ] text-string ] | [ { secret [ 0 | 5 ] text-string } ] ]
```


```
no username name
```


Parameter Description	Parameter	Description
	<i>name</i>	Username
	<b>login mode</b>	Sets the login mode.
	<b>console</b>	Sets the login mode to console.
	<b>ssh</b>	Sets the login mode to ssh.
	<b>telnet</b>	Sets the login mode to telnet.
	<b>online amount</b> <i>number</i>	Sets the amount of users online simultaneously.
	<b>permission</b> <i>oper-mode path</i>	Sets the permission on the specified file. <i>oper-mode</i> refers to the operation mode and <i>path</i> to the file or the directory path.
	<b>privilege</b> <i>privilege-level</i>	Sets the privilege level, in the range from 0 to 15.
	<b>reject remote-login</b>	Confines the account to remote login.
	<b>web-auth</b>	Confines the account to web authentication.
	<b>pwd-modify</b>	Allows the web authentication user of this account to change the password. It works only when the <b>web-auth</b> command is configured.
	<b>nopassword</b>	The account is not configured with a password.
	<b>password</b> [ 0   7 ] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted. The password is in plain text by default.
	<b>secret</b> [ 0   7 ] <i>text-string</i>	Configures a secure password for the account. The password configured by this command is stored as a ciphertext password after irreversible encryption. <b>0</b> indicates that a plaintext password is entered, <b>5</b> indicates that a password encrypted using the MD5 algorithm is entered, <b>8</b> indicates that a password encrypted using the SHA-256 algorithm is entered. A plaintext password is entered by default.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to establish a local user database for authentication. The cleartext password can be configured in interactive mode.

 If encryption type is 7, the cipher text you enter should contain seven characters to be valid. In general, do not set the encryption type 7.

 Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.

**Configuration Examples** The following example configures a username and password and binds the user to level 15.

```
Hostname(config)# username test privilege 15 password 0 pw15
```

The following example configures the username and password exclusive to web authentication.

```
Hostname(config)# username user1 web-auth password 0 pw
```

The following example configures user test with read and write permissions on all files and directories.

```
Hostname(config)# username test permission rw /
```

The following example configures user test with read, write and execute permissions on all files and directories except the config.text file.

```
Hostname(config)# username test permission n /config.text
Hostname(config)# username test permission rwx /
```

#### Related Commands

Command	Description
<b>login local</b>	Enables local authentication

#### Platform

N/A

#### Description

## 1.70 username import

Use this command to import user information from the file.

**username import** *filename*

#### Parameter Description

Parameter	Description
<i>filename</i>	The file name.

#### Defaults

N/A

#### Command Mode

Privileged EXEC mode

#### Usage Guide

This command is used to import user information from the file.

#### Configuration Examples

The following example imports user information from the file.

```
Hostname# username import user.csv
```

#### Related Commands

Command	Description
N/A	N/A

#### Platform

N/A

#### Description

## 1.71 username export

Use this command to export user information to the file.

**username export** *filename*

Parameter Description	Parameter	Description
	<i>filename</i>	The file name.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to export user information to the file.

**Configuration** The following example exports user information to the file.

**Examples**

```
Hostname# username export user.csv
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.72 write

Use this command to save **running-config** at a specified location.

**write** [ **memory** | **terminal** ]

Parameter Description	Parameter	Description
	<b>memory</b>	Writes the system configuration (running-config) into NVRAM, which is equivalent to <b>copy running-config startup-config</b> .
	<b>terminal</b>	Displays the system configuration, which is equivalent to <b>show running-config</b> .

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations.

The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists;

The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device such as USB drive, and the device has not been loaded when you run the **write [ memory ]** command.

**Configuration** The following example saves **running-config** at a specified location.

**Examples**

```
Hostname# write
Building configuration
[OK]
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

# 1 Line Commands

## 1.1 access-class

Use this command to control login into the terminal through IPv4 ACL. Use the **no** form of this command to restore the default setting.

**access-class** { *access-list-number* | *access-list-name* } { **in** | **out** }

**no access-class** { *access-list-number* | *access-list-name* } { **in** | **out** }

Parameter Description	Parameter	Description
	<i>access-list-number</i>	Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699.
	<i>access-list-name</i>	Specifies the ACL name.
	<b>in</b>	Filters the incoming connections.
	<b>out</b>	Filters the outgoing connections.

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example uses ACL 20 to filter the incoming connections in line VTY 0 5.

```
Hostname(config)# line vty 0 5
Hostname(config-line)access-list 20 in
```

The following example uses the ACL named "test" to filter the outgoing connections in line VTY 6 7.

```
Hostname(config)# line vty 6 7
Hostname(config-line)access-list test out
```

Related Commands	Command	Description
	<b>show running</b>	Displays status information

**Platform Description** N/A



## 1.2 accounting exec

Run the **accounting exec** command to configure the user EXEC accounting method list for a line.

**accounting exec** { **default** | *list-name* }

Run the **no** form of this command to remove this configuration.

**no accounting exec**

### Parameter Description

Parameter	Description
<b>default</b>	Specifies the name of the default authentication method list.
<i>list-name</i>	Name of the optional method list.

### Defaults

No user EXEC accounting method list is configured for a line by default.

### Command Mode

Line configuration mode

### Usage Guide

This command is used with AAA. After the EXEC accounting method is configured, apply it to a line.

### Configuration Examples

The following example sets the user EXEC accounting method list to the default method list for VTY 1.

```

Hostname(config)# aaa new-model
Hostname(config)# aaa accounting exec default start-stop group radius
Hostname(config)# line vty 1
Hostname(config-line)# accounting exec default

```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.3 authorization commands

Use this command to enable authorization on commands, Use the **no** form of this command to restore the default setting.

**authorization commands** *level* { **default** | *list-name* }

**no authorization commands** *level*

Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
	<b>default</b>	Default authorization list name,
	<i>list-name</i>	Optional list name.

**Defaults** This function is disabled by default.

**Command Mode** Line configuration mode

**Usage Guide** This function is used together with AAA authorization. Configure AAA authorization first, and then apply it on the line.

**Configuration Examples** The following example enables authorization on commands of level 15 in line VTY 1.

```

Hostname(config)# aaa new-model
Hostname(config)# aaa authorization commands 15 default group tacacs+
Hostname(config)# line vty 1
Hostname(config-line)# authorization commands 15 default

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.4 authorization exec

Use this command to enable EXEC authorization for the line. Use the **no** form of this command to restore the default setting.

**authorization { default | list-name }**

**no authorization exec**

Parameter Description	Parameter	Description
	<b>default</b>	Default authorization list name,
	<i>list-name</i>	Optional list name.

**Defaults** This function is disabled by default,

**Command** Line configuration mode  
**Mode**

**Usage Guide** This function is used together with AAA authorization. Configure AAA EXEC authorization first, and then apply it on the line.

**Configuration** The following example performs EXEC authorization to line VTY 1.

**Examples**

```

Hostname(config)# aaa new-model
Hostname(config)# aaa authorization exec default group radius
Hostname(config)# line vty 1
Hostname(config-line)# authorization exec default
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.5 clear line

Use this command to clear connection status of the line.  
**clear line** { **console** *line-num* | **vtty** *line-num* | *line-num* }

**Parameter Description**

Parameter	Description
<b>console</b>	Clears connection status of the console line.
<b>vtty</b>	Clears connection status of the virtual terminal line.
<i>line-num</i>	Specifies the line to be cleared.

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** This command is used to clear connection status of the line and restore the line to the unoccupied status to create new connections.

**Configuration** The following example clears connection status of line VTY 13. The connected session on the client (such as Telnet and SSH) in the line is disconnected immediately.

**Examples**

```

Hostname# clear line vty 13
    
```

**Related Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

**Platform** N/A  
**Description**

## 1.6 disconnect-character

Use this command to set the hot key that disconnects the terminal service connection. Use the **no** form of this command to restore the default setting.

**disconnect-character** *ascii-value*

**no disconnect-character**

Parameter Description	Parameter	Description
	<i>ascii-value</i>	ASCII decimal value of the hot key that disconnects the terminal service connection, in the range from 0 to 255.

**Defaults** The default hot key is **Ctrl+D** and the ASCII decimal value is 0x04.

**Command Mode** Line configuration mode

**Usage Guide** This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service cannot operate properly.

**Configuration Examples** The following example sets the hot key that disconnects the terminal service connection on line VTY 0 5 to **Ctrl+E** (0x05).

```

Hostname(config)# line vty 0 5
Hostname(config-line)# disconnect-character 5

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.7 escape-character

Use this command to set the escape character for the line. Use the **no** form of this command to restore the default setting.

**escape-character** *escape-value*

**no escape-character****Parameter  
Description**

Parameter	Description
<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the line, in the range from 0 to 255.

**Defaults** The default escape character is **Ctrl+^ (Ctrl+Shift+6)** and the ASCII decimal value is 30.

**Command  
Mode** Line configuration mode

**Usage Guide** After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

**Configuration Examples** The following example sets the escape character for the line to 23 (**Ctrl+w**).

```

Hostname(config)# line vty 0
Hostname(config-line)# escape-character 23

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.8 exec

Use this command to enable the line to enter the command line interface. Use the **no** form of this command to disable the function.

**exec**

**no exec**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** This function is enabled by default.

**Command  
Mode** Line configuration mode

**Usage Guide** The **no exec** command is used to ban the line from entering the command line interface. You have to enter the command line interface through other lines,

**Configuration** The following example bans line VTY 1 from entering the command line interface.

```

Examples
Hostname(config)# line vty 1
Hostname(config-line)# no exec
Hostname# show users
Line          User          Host(s)          Idle           Location
-----
-----
* 0 con 0     ---          idle            00:00:00     ---
  1 vty 0     ---          idle            00:01:03     20.1.1.2
  3 vty 2     ---          idle            00:00:13     20.1.1.2
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 history

Use this command to enable command history for the line or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

**history [ size size ]**

**no history**

**no history size**

Parameter Description	Parameter	Description
	<b>size size</b>	

**Defaults** This function is enabled by default, The default *size* is 10.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the number of commands in the command history to 20 for line VTY 0 5.

```

Examples
Hostname(config)# line vty 0 5
Hostname(config-line)# history size 20

The following example disables the command history for line VTY 0 5.
Hostname(config)# line vty 0 5
    
```

```
Hostname(config-line)# no history
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.10 ipv6 access-class

Use this command to configure access to the terminal through IPv6 ACL. Use the **no** form of this command to restore the default setting.

```
ipv6 access-class access-list-name { in | out }
no ipv6 access-class access-list-name { in | out }
```

<b>Parameter Description</b>	Parameter	Description
	<i>access-list-name</i>	Specifies the ACL name.
	<b>in</b>	Filters the incoming connections.
	<b>out</b>	Filters the outgoing connections.

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example uses the ACL named “test” to filter the outgoing IPv6 connections in line VTY 0 4.

```
Hostname(config)# line vty 0 4
Hostname(config-line)ipv6 access-class test out
```

<b>Related Commands</b>	Command	Description
	<b>show running</b>	Displays status information

**Platform** N/A  
**Description**

## 1.11 length

Use this command to set the screen length for the line. Use the **no** form of this command to restore the default setting.

**length** *screen-length*

**no length**

### Parameter Description

Parameter	Description
<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.

### Defaults

The default is 24.

### Command Mode

Line configuration mode

### Usage Guide

N/A

### Configuration Examples

The following example sets the screen length to 10.

```
Hostname(config-line)# length 10
```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.12 line

Use this command to enter the specified LINE mode.

**line** [*console* | *vtty* ] *first-line* [ *last-line* ]

### Parameter Description

Parameter	Description
<b>console</b>	Console port
<b>vtty</b>	Virtual terminal line, applicable for telnet/ssh connection.
<i>first-line</i>	Number of first line to enter
<i>last-line</i>	Number of last line to enter

### Defaults

N/A



**Command** Global configuration mode  
**Mode**

### Usage Guide

**Configuration** The following example enters the LINE mode from LINE VTY 1 to 3:

**Examples**

```
Hostname(config)# line vty 1 3
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.13 line vty

Use this command to increase the number of VTY connections currently available. Use the **no** form of this command to restore the default setting.

**line vty** *line-number*

**no line vty** *line-number*

Parameter Description	Parameter	Description
	<i>line-number</i>	

**Defaults** By default, there are five available VTY connections, numbered 0 to 4.

**Command** Global configuration mode.  
**Mode**

### Usage Guide

**Configuration** The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19.

```
Hostname(config)# line vty 19
```

Decrease the number of available VTY connections to 10. The available VTY connections are numbered 0-9.

```
Hostname(config)# line vty 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.14 location

Use this command to configure the line location description. Use the **no** form of this command to restore the default setting.

**location** *location*  
**no location**

Parameter Description	Parameter	Description
	<i>location</i>	Line location description

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example describes the line location as Swtich's Line VTY 0.

```

Hostname(config)# line vty 0
Hostname(config-line)# location Swtich's Line Vty 0
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.15 monitor

Use this command to enable log display on the terminal. Use the **no** form of this command to restore the default setting,

**monitor**  
**no monitor**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example enables log display on the terminal in VTY line 0 5.

```

Examples
Hostname(config)# line vty 0 5
Hostname(config-line)# monitor

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.16 privilege level

Use this command to set the privilege level for the line. Use the **no** form of this command to restore the default setting.

**privilege level** *level*  
**no privilege level**

Parameter Description	Parameter	Description
	<i>level</i>	

**Defaults** The default is 1.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the privilege level for the line VTY 0 4 to 14.

```

Examples
Hostname(config)# line vty 0 4
Hostname(config-line)privilege level 14

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.17 refuse-message

Use this command to set the login refusal message for the line. Use the **no** form of this command to restore the default setting.

**refuse-message** [ *c message c* ]

**no refuse-message**

Parameter Description	Parameter	Description
	<i>c</i>	Delimiter of the login refusal message, which is not allowed within the message.
	<i>message</i>	Login refusal message.

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** This command is used to set the login refusal message for the line. The characters entered after the ending delimiter are discarded directly, The login refusal message is displayed when the user has been refused to login.

**Configuration Examples** The following example sets the login refusal message for the line to "Unauthorized user cannot login to the device".

```
Hostname(config-line)#vacant-message @ Unauthorized user cannot login to
the device @
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.18 show history

Use this command to display the command history of the line.

**show history**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration</b>	The following example displays the command history of the line.	
<b>Examples</b>	<pre> Hostname# show history exec: sh privilege sh run show user sh user all show history </pre>	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.19 show line

Use this command to display line configuration.

**show line** { **console** *line-num* | **vtty** *line-num* | *line-num* }

<b>Parameter Description</b>	Parameter	Description
	<b>console</b>	Displays configuration for the console line.
	<b>vtty</b>	Displays configuration for the virtual terminal line.
	<i>line-num</i>	Displays the line.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	

**Configuration** The following example displays configuration for the console port.

**Examples**

```

Hostname# show line console 0
CON    Type    speed  Overruns
* 0    CON     9600  45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape Disconnect Activation
              ^^x    none      ^M
Timeouts:     Idle EXEC    Idle Session
              never      never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output: 395756 bytes
Data overflow: 27697 bytes
stop rx interrupt: 0 times
    
```

Field	Description
CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.
Type	Terminal type, including CON and VTY.
speed	Asynchronous speed.
Overruns	The number of overrun errors received by the flash.
Line 0	Terminal line number.
Location: ""	Line location configuration.
Type: "vt100"	Compatibility standard.
Special Chars	Special characters, including Escape, Disconnect, and Activation characters.
Timeouts	Timeout value; "never" indicates no timeout.
History	Whether to enable command history; the number of commands in the command history.
Total input	Data volume received from the drive.
Total output	Date volume sent to the drive.
Data overflow	Overflowing data volume.
stop rx interrupt	Data reception interruption times.

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.20 show privilege

Use this command to display the privilege level of the line.

**show privilege**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the privilege level of the line.

**Examples**

```

Hostname# show privilege
Current privilege level is 10

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.21 show users

Use this command to display the login user information.

**show users [ all ]**

Parameter Description	Parameter	Description
	all	Displays line user information, including users logging into the line and users not logging into the line.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the information about users logging into the line,

**Examples**

```

Hostname# show users
Line          User          Host(s)          Idle          Location
-----
0 con 0      ---          idle            00:00:46     ---
1 vty 0      ---          idle            00:00:29     20.1.1.2
* 2 vty 1    ---          idle            00:00:00     20.1.1.2
    
```

The following example displays all line user information,

```

Hostname(config)# show users all
Line          User          Host(s)          Idle          Location
-----
0 con 0      ---          idle            00:00:49     ---
1 vty 0      ---          idle            00:00:32     20.1.1.2
* 2 vty 1    ---          idle            00:00:00     20.1.1.2
3 vty 2      ---          idle            00:00:00     ---
4 vty 3      ---          idle            00:00:00     ---
5 vty 4      ---          idle            00:00:00     ---
6 vty 5      ---          idle            00:00:00     ---
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.22 speed

Use this command to configure the baud rate for the specified line. Use the **no** form of this command to restore the default setting,

**speed** *baudrate*

**no speed**

**Parameter Description**

Parameter	Description
<i>baudrate</i>	Sets the baud rate, in the range from 9600 to 115200.

**Defaults** The default is 9600.

**Command Mode** LINE configuration mode



**Usage Guide** N/A

**Configuration** The following example sets the baud rate to 115200,

**Examples**

```
Hostname(config-line)# speed 115200
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.23 terminal escape-character

Use this command to set the escape character for the current terminal. Use the **no** form of this command to restore the default setting.

**terminal escape-character** *escape-value*

**terminal no escape-character**

**Parameter  
Description**

Parameter	Description
<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255.

**Defaults** The default escape character is **Ctrl+^ (Ctrl+Shift+6)** and the ASCII decimal value is 30.

**Command  
Mode** Privileged EXEC mode

**Usage Guide** After configuring this command, press the key combination of the escape character and then press **x**, the current session is disconnected to return to the original session.

**Configuration** The following example sets the escape character for the current terminal to 23 (**Ctrl+w**).

**Examples**

```
Hostname# terminal escape-character 23
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.24 terminal history

Use this command to enable command history for the current terminal or set the number of commands in the command history. Use the **no history** command to disable command history. Use the **no history size** command to restore the number of commands in the command history to the default setting.

**terminal history** [ **size** *size* ]

**terminal no history**

**terminal no history size**

Parameter Description	Parameter	Description
	<b>size</b> <i>size</i>	Sets the number of commands, in the range from 0 to 256.

**Defaults** This function is enabled by default, The default *size* is 10.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the number of commands in the command history to 20 for the current terminal.

```
Hostname# terminal history size 20
```

The following example disables the command history for the current terminal.

```
Hostname# terminal no history
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.25 terminal length

Use this command to set the screen length for the current terminal. Use the **no** form of this command to restore the default setting.

**terminal length** *screen-length*

**terminal no length**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.
----------------------	---

**Defaults** The default is 24.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the screen length for the current terminal to 10.

```
Hostname# terminal length 10
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.26 terminal location

Use this command to configure location description for the current device. Use the **no** form of this command to restore the default setting.

**terminal location** *location*

**terminal no location**

**Parameter Description**

Parameter	Description
<i>location</i>	Configures location description of the current device.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example configures location description of the current device as "Switch's Line Vty 0".

```
Hostname# terminal location Switch's Line Vty 0
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.27 terminal speed

Use this command to configure the baud rate for the current terminal. Use the **no** form of this command to restore the default setting,

**terminal speed** *baudrate*

**terminal no speed**

Parameter Description	Parameter	Description
	<i>baudrate</i>	Sets the baud rate, in the range from 9600 to 115200.

**Defaults** The default is 9600.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the baud rate for the current terminal to 115200,

```
Hostname# terminal speed 115200
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.28 terminal width

Use this command to set the screen width for the terminal.

**terminal width** *screen-width*

**terminal no width**

Parameter Description	Parameter	Description
	<i>screen-width</i>	Sets the screen width for the terminal, in the range from 0 to 256.

**Defaults** The default is 79.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example sets the screen width for the terminal to 10.

**Examples**

```
Hostname# terminal width 10
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.29 timeout login response

Use this command to set the login authentication timeout for the line. Use the **no** form of this command to restore the default setting.

**timeout login response** *seconds*

**no timeout login response**

**Parameter Description**

Parameter	Description
<b>response</b>	The time period during which the line waits for the user to enter any message.
<i>seconds</i>	Timeout value, in the range from 1 to 300 in the unit of seconds.

**Defaults** The default is 30.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the login authentication timeout to 300 seconds for line VTY 0 5.

**Examples**

```
Hostname(config)# line vty 0 5
Hostname(config-line) timeout login response 300
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.30 transport input

Use this command to set the specified protocol under Line that can be used for communication. Use the **no** form of this command to restore the default setting.

**transport input** { **all** | **ssh** | **telnet** | **none** }

**no transport input** { **all** | **ssh** | **telnet** | **none** }

Parameter Description	Parameter	Description
	<b>all</b>	Allows all the protocols under Line to be used for communication
	<b>ssh</b>	Allows only the SSH protocol under Line to be used for communication
	<b>telnet</b>	Allows only the Telnet protocol under Line to be used for communication
	<b>none</b>	Allows none of protocols under Line to be used for communication

**Defaults** **all**, **ssh** and **telnet** protocols are allowed.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example specifies that only the Telnet protocol is allowed to login in line vty 0 4.

```
Hostname(config)# line vty 0 5
Hostname(config-line)transport input ssh
```

Related Commands	Command	Description
	<b>show running</b>	Displays status information

**Platform** N/A  
**Description**

## 1.31 vacant-message

Use this command to set the logout message. Use the **no** form of this command to restore the default setting.

**vacant-message** [ *c message c* ]

**no vacant-message**

Parameter Description	Parameter	Description
	<i>c</i>	Delimiter of the logout message, which is not allowed within the message.
	<i>message</i>	Logout message.

**Defaults** N/A

**Command Mode** Line configuration mode

**Usage Guide** This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly, The logout message is displayed when the user logs out.

**Configuration** The following example sets the logout message to "Logout from the device".

**Examples**

```
Hostname(config-line)#vacant-message @ Logout from the device @
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.32 width

Use this command to set the screen width for the line. Use the **no** form of this command to restore the default setting,

**width** *screen-width*

**no width**

Parameter Description	Parameter	Description
	<i>screen-width</i>	Sets the screen width for the line, in the range from 0 to 256,

**Defaults** The default is 79.

**Command Mode** Line configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the screen width for the line to 10.

**Examples** `Hostname(config-line)# width 10`

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A



# 1 File System Commands

## 1.1 cd

Use this command to set the present directory for the file system.

**cd** [ *filesystem:* ] [ *directory* ]

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of filesystem, followed by a colon (:). The filesystem includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
	<i>directory</i>	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

**Defaults** The default directory is the flash root directory.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide**

**Configuration** The following example enters the sata hardware.

**Examples**

```

Hostname#pwd
flash:/
Hostname#cd sata:
Hostname#pwd
sata:/
    
```

Related Commands	Command	Description
	<b>pwd</b>	Displays the present word directory.

**Platform** N/A.

**Description**

## 1.2 copy

Use this command to copy a file from the specified source directory to the specified destination directory.

**copy** *source-url destination-url*

Parameter	Parameter	Description
Description	<i>source-url</i>	Source file URL, which can be local or remote.
	<i>destination-url</i>	Destination file URL, which can be local or remote.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** when the file to be copied exists on the target URL, the target file system determines the action, such as error report, overwrite, or offering you the choice.

The following table lists the URL:

Prefix	Description
<b>running-config</b>	Running configuration file.
<b>startup-config</b>	startup configuration file.
<b>flash:</b>	local FLASH file system.
<b>tftp:</b>	The URL of TFTP network server, in the format as follows: <b>tftp:[[/location]/directory]/filename</b>

**Configuration Examples** The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfig file exists locally.

```

Hostname#copy tftp://192.168.64.2/netconfig flash:/netconfig
Do you want to overwrite [/data/netconfig]? [Y/N]:y
Press Ctrl+C to quit
!
Copy success.
    
```

**Related Commands**

Command	Description
<b>delete</b>	Deletes the file.
<b>rename</b>	Renames the file.
<b>dir</b>	Displays the file list of the specified directory.

**Platform Description** N/A

### 1.3 delete

Use this command to delete the files in the present directory.

**delete** [ *filesystem:* ] *file-url*

Parameter	Description
<b>Description</b> <i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash: sata:, usb:, sd:, tmp:.</b>

<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
-----------------	---

**Defaults** The default *filesystem:* is **flash:**.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide**

**Configuration** The following example deletes the fstab file on the FLASH disk.

```

Examples
Hostname#pwd
flash:/
Hostname#dir
Directory of flash:/
1  -rw-      336   Jan 03 2012 18:53:42  fstab
2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Hostname#delete flash:/fstab
Do you want to delete [flash:/fstab]? [Y/N]:y
Delete success.
Hostname#dir
Directory of flash:/
1  -rw-      4096   Jan 03 2012 12:32:09  rc.d
2  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
2 files, 0 directories

10,489,856 bytes total (13,192,992 bytes free)
    
```

<b>Related Commands</b>	Command	Description
	<b>copy</b>	Copies the file.
	<b>dir</b>	Displays the file list of the specified directory.

**Platform** N/A  
**Description**

## 1.4 dir

Use this command to display the files in the present directory.

**dir** [ *filesystem:* ] [ *directory* ]

Parameter	Description
-----------	-------------

<b>Parameter</b>	<i>filesystem</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
<b>Description</b>	<i>directory</i>	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

**Defaults** By default, only the information under the present working path is displayed.

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration** The following example displays the file information of the root directory in the FLASH disk.

**Examples**

```

Hostname#dir flash:/
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
    
```

Field	Description
1, 2, 3	Index number
-rw-	Permissions on a file include: <ul style="list-style-type: none"> <li>● d: directory</li> <li>● r: read</li> <li>● w: write</li> <li>● x: executable</li> </ul>
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

**Related**

**Commands**

Command	Description
<b>pwd</b>	Displays the present directory.
<b>cd</b>	Sets the present directory of the file system.

**Platform** N/A.

**Description**

## 1.5 eject

Use this command to offload the USB flash drive or SD.

**eject [ usb0 | sd0 ]**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example unmounts the USB device.

```

Hostname#eject ?
sd0   Eject sd disk 0
usb0  Eject usb disk 0

Hostname#eject usb0
Hostname#
    
```

**Verification** Run the **show mount** command.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.6 erase

Use this command to erase the device or file that doesn't have a file system.

**erase filesystem**

Parameter	Parameter	Description
Description	<i>filesystem:</i>	Name of the file system, followed by a colon (:).

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example erases the USB filesystem.

**Examples**

```
Hostname#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 ...
Erase disk usb0 done!
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.7 mkdir

Use this command to create a directory.

**mkdir** [ *filesystem:* ] *directory*

Parameter	Parameter	Description
<b>Description</b>	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
	<i>directory</i>	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

**Defaults** The default *filesystem:* is **flash:**.  
The default *directory* is the root directory.

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration** The following example creates a directory named newdir:

**Examples**

```
Hostname#dir
Directory of flash:/
1  -rw-      336   Jan 03 2012 18:53:42  fstab
2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
Hostname#mkdir newdir
```

```
Created dir flash:/newdir
Hostname#dir
Directory of flash:/
1  -rw-      336   Jan 03 2012 18:53:42  fstab
2  -rw-      4096  Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760  Jan 03 2012 18:13:37  rpmdb
4  drw-      4096  Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

**Related Commands**

Command	Description
<b>rmdir</b>	Deletes the directory.
<b>pwd</b>	Displays the present directory.

**Platform** N/A  
**Description**

## 1.8 more

Use this command to display the content of a file.

```
more [ /ascii | /binary ] [ filesystem: ] file-url
```

**Parameter Description**

Parameter	Description
<b>/ascii</b>	Displays the file content in the ASCII format.
<b>/binary</b>	Displays the file content in the
<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

**Defaults** The file is displayed in its own format by default.

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the content of the netconfig file under root directory of FLASH disk.

```
Hostname#more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
```

```
#
#      <network_id> <semantics> <flags> <protofamily> <protoname> \
#      <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp      tpi_clts      v      inet      udp      -      -
tcp      tpi_cots_ord v      inet      tcp      -      -
udp6     tpi_clts      v      inet6     udp      -      -
tcp6     tpi_cots_ord v      inet6     tcp      -      -
rawip    tpi_raw        -      inet      -      -      -
local    tpi_cots_ord -      loopback  -      -      -
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 pwd

Use this command to display the working path.

**pwd**

Parameter Description	Parameter	Description
	N/A.	N/A.

**Defaults** N/A.

### Usage Guide

**Configuration** The following example displays the process of switching the working directory from flash: to sata:.

**Examples**

```
Hostname#pwd
flash:/
Hostname#cd sata:/
Hostname#pwd
sata:/
```

Related Commands	Command	Description
	cd	Changes the file system in the present directory.



**Platform** N/A.  
**Description**

## 1.10 rename

Use this command to move or rename the specified file.

**rename** *src-url dst-url*

Parameter	Parameter	Description
<b>Description</b>	<i>src-url</i>	The source file URL to move.
	<i>dst-url</i>	The URL of the destination file or directory.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example renames the fstab file in the root directory on the FLASH disk as new-fstab.

**Examples**

```

Hostname#dir
Directory of flash:/
1  -rw-      336   Jan 03 2012 18:53:42  fstab
2  -rw-      4096  Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760  Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Hostname#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
Hostname#dir
Directory of flash:/
1  -rw-      336   Jan 03 2012 18:53:42  new-fstab
2  -rw-      4096  Jan 03 2012 12:32:09  rc.d
3  -rw-  10485760  Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
    
```

Related Commands	Command	Description
	<b>delete</b>	Deletes the file.
	<b>copy</b>	Copies the file.

**Platform** N/A  
**Description**

## 1.11 rmdir

Use this command to delete an empty directory.

**rmdir** [ *filesystem:* ] *directory*

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
	<i>directory</i>	The path name. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.

**Defaults** The default *filesystem:* is **flash:**.

**Command** Privileged EXEC mode.

**Mode**

### Usage Guide

**Configuration** The following example deletes the null test directories.

### Examples

```

Hostname#mkdir newdir
Hostname#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
 4  drw-      4096   Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
Hostname#rmdir newdir
removed dir flash:/newdir
Hostname#dir
Directory of flash:/
 1  -rw-      336   Jan 03 2012 18:53:42  fstab
 2  -rw-     4096   Jan 03 2012 12:32:09  rc.d
 3  -rw-  10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
    
```

Related Commands	Command	Description
	N/A.	N/A.

**Platform** N/A.

**Description**

## 1.12 show file systems

Use this command to display the file system information.

### show file systems

Parameter	Parameter	Description
Description	N/A.	N/A.

**Defaults** N/A.

**Command Mode** User EXEC mode, privileged EXEC mode, global configuration mode, and interface configuration mode

**Usage Guide** Use this command to display the file systems supported in the present devices and the available space condition in the file system.

**Configuration** The following example displays the file system information:

#### Examples

```

Hostname#show file systems
  Size(KB)      Free(KB)      Type  Flags Prefixes
    NA           NA        ram   rw tmp:
    NA           NA    network  rw tftp:
    NA           NA    network  rw oob_tftp:
    8192         2416        disk   rw flash:
167772160     147772160        disk   rw sata0:
  1048576       548576        disk   rw usb0:
   262144      152144        disk   rw sd0:
    
```

Field	Description
Size(KB)	File system space, in the unit of KB.
Free(KB)	Available file system space, in the unit of KB.
Type	File system type
Flags	Permissions on the file system include: <ul style="list-style-type: none"> <li>● ro: read-only</li> <li>● wo: write-only</li> <li>● rw: read and write</li> </ul>
Prefixes	File system prefix

Related Commands	Command	Description
	N/A.	N/A.

**Platform** N/A.

#### Description

## 1.13 show mount

Use this command to display the mounted information.

**show mount**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** User EXEC mode, privileged EXEC mode, global configuration mode, and interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the mounted information.

**Examples**

```

Hostname#show mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc
(rw,noexec,nosuid,nodev)
    
```

Field	Description
proc	Source address of mount.
on	-
/proc	Destination address of mount.
type	-
proc	Mount type.
(rw,noexec,nosuid,nodev)	Mount property.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.14 tree

Use this command to display the file tree of the current directory.

**tree** [ *filesystem:* ] [ *directory* ]

Parameter	Parameter	Description
<b>Description</b>	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

**Defaults** The default *filesystem:* is **flash:**.

**Command Mode** User EXEC mode and privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the file tree of flash:/echo

```

Hostname#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
|   +-- echo.ko
|   +-- echo.mod.c
|   +-- echo.mod.o
|   +-- echo_module.c
|   +-- echo_module.o
|   +-- echo.o

```

```

|   +-- echo_server.c
|   +-- echo_server.o
|   +-- echo_sysfs.c
|   +-- echo_sysfs.h
|   +-- echo_sysfs.o
|   +-- Makefile
|   +-- modules.order
|   +-- Module.symvers
|   +-- msg_fd.c
|   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
+-- user_space
    +-- echo_server.c
    +-- echo_server.o
    +-- Makefile
    +-- msg_fd.c
+-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
    
```

Related	Command	Description
Commands	N/A	N/A

Platform N/A

Description

### 1.15 verify

Use this command to compute, display, and verify Message Digest 5 (MD5).

**verify** [ /md5 md5-value ] filesystem: [ file-url ]

Parameter	Parameter	Description
Description	<b>/md5</b>	Computes and displays MD5.
	<b>md5-value</b>	The file MD5, which is compared with the computed MD5.
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes <b>flash:</b> , <b>sata:</b> , <b>usb:</b> , <b>sd:</b> , <b>tmp:</b> .
	<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.

**Defaults** The default *filesystem:* is **flash:**.

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example computes the MD5 value of **flash:/gcc**.

**Examples**

```
Hostname#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

The following example computes the MD5 value of **flash:/gcc** and makes a comparison.

```
Hostname#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying flash:/gcc = 8b072de7db7affd8b2ef824e7e4d716c
Hostname#verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc
%Error verifying flash:/gcc
Computed signature = 8b072de7db7affd8b2ef824e7e4d716c
Submitted signature = 8b072de7db7affd8b2ef824e7e4d71
```

**Related**

**Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

# 1 HTTP Commands

## 1.1 enable service web-server

Use this command to enable the HTTP service function.

Use the **no** or **default** form of this command to disable the HTTP service function.

**enable service web-server** [ **http** | **https** | **all** ]

**no enable service web-server** [ **http** | **https** ]

**default enable service web-server** [ **http** | **https** ]

### Parameter Description

Parameter	Description
<b>http</b>	Enables the HTTP service.
<b>https</b>	Enables the HTTPS service.
<b>all</b>	Enables both the HTTP service and the HTTPS service.

### Defaults

By default, the HTTP service function is disabled.

### Command mode

Global configuration mode.

### Usage Guide

If run a command ends with the keyword **all** or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword **http**, it indicates enabling the HTTP service; if run a command ends with keyword **https**, it indicates enabling the HTTPS service. Use the command **no enable service web-server** to disable the corresponding HTTP service.

### Configuration

The following example enables both the HTTP service and the HTTPS service:

### Examples

```
Hostname#configure terminal
Hostname(config)#enable service web-server
```

### Verification

Use the **show service** command to display the service status.

Use the **show web-server status** command to display the status of the web service.

### Notifications

If the port is 80 and the HTTP service fails, the following notification will be displayed:

```
%notice:Failed to open tcp listen, port=[80].
```

### Related Commands

Command	Description
N/A	N/A



**Platform** N/A

**Description**

## 1.2 http port

Use this command to configure the HTTP port number.

Use the **no** form of this command to restore the default HTTP port number.

**http port** *port-number*

**no http port**

**Parameter  
Description**

Parameter	Description
<i>port-number</i>	Configures the HTTP port number. The value includes 80, 1025 to 65,535.

**Defaults**

The default HTTP port number is 80.

**Command  
mode**

Global configuration mode.

**Usage Guide**

Use this command to configure the HTTP port number.

**Configuration**

The following example configures the HTTP port number as 8080:

**Examples**

```
Hostname(config)#http port 8080
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.3 http secure-port

Use this command to configure the HTTPS port number.

Use the **no** form of this command to restore the default HTTPS port number.

**http secure-port** *port-number*

**no http secure-port**

**Parameter  
Description**

Parameter	Description
<i>port-number</i>	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.

- Defaults** The default HTTP port number is 443.
- Command mode** Global configuration mode.
- Usage Guide** Use this command to configure the HTTPS port number.

**Configuration** The following example configures the HTTPS port number as 4443:

**Examples**

```
Hostname#configure terminal
Hostname(config)#http secure-port 4443
```

**Related Commands**

Command	Description
<b>enable service web-server</b>	Enables the HTTP service.
<b>show web-server status</b>	Displays the configuration and status of the Web service.

- Platform** N/A
- Description**

## 1.4 show web-server https certificate information

Use this command to display information about the HTTPS service certificate.

**show web-server https certificate information**

**Parameter Description**

Parameter	Description
N/A	N/A

- Defaults** N/A

- Command mode** All modes except the user EXEC mode

- Usage Guide** N/A

**Configuration** The following example displays information about the HTTPS service certificate.

**Examples**

```
Hostname# show web-server https certificate information
Source: Default
Certificate:
  Data:
    Version: 3 (0x2)
```

```
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=Self-Signed-CA472E87
Validity
  Not Before: Feb 20 07:26:51 2019 GMT
  Not After : Feb 17 07:26:51 2029 GMT
Subject: CN=Self-Signed-CA472E87
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
  Modulus:
    00:ec:39:13:5a:09:da:97:d1:83:8f:a7:77:cf:b4:
    88:96:a0:85:23:68:4d:5a:c6:d3:4b:d9:c0:d6:1b:
    f4:42:29:ce:33:2e:2f:79:5e:cc:bb:bd:5f:63:5b:
    41:f3:9f:fb:82:c7:ca:8a:21:a9:c2:fb:36:db:62:
    08:3c:05:b8:a2:47:07:1a:20:99:80:24:63:a4:08:
    66:22:86:b6:aa:46:43:8a:91:7d:99:f3:8a:7c:58:
    ac:1f:ef:6c:4c:d1:d6:bf:ef:a1:77:64:4b:53:16:
    29:2f:1c:e8:ec:d6:6b:b6:34:64:32:00:1f:09:30:
    69:8d:2e:85:d5:6a:db:45:cb:b8:fd:38:ba:bd:68:
    1d:de:38:65:ef:3f:c6:90:bf:ca:1a:9e:df:c3:75:
    5f:20:bd:61:b4:bd:43:6b:77:ef:25:c6:43:0a:0f:
    dc:5a:0e:28:53:37:14:77:8b:bd:ea:14:54:c5:e1:
    45:27:c9:14:63:37:67:bc:0f:09:15:1f:73:ae:bb:
    46:b1:ad:cd:23:89:fd:2c:0c:9f:a3:34:62:f0:14:
    0d:c8:92:09:68:df:8f:69:fb:1c:49:91:d8:1c:f7:
    ee:67:a3:25:c5:9a:e2:f6:1c:a8:8c:af:7e:08:29:
    44:32:b1:d8:a9:86:04:a2:80:65:24:47:56:f4:fd:
    e4:19
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
Signature Algorithm: sha256WithRSAEncryption
  16:b8:e2:1e:45:13:56:9c:48:ef:ec:40:fb:9a:e3:4c:da:e4:
  95:c4:3b:92:10:9a:27:a0:da:ab:45:86:4c:39:fd:73:0c:e8:
  98:8b:0e:a4:28:72:66:0a:74:cc:9c:91:71:2f:94:dd:4b:4b:
  a2:54:e5:8f:47:82:bd:82:4d:70:93:6e:af:72:ce:cf:db:e2:
  36:b1:64:1a:1f:5e:c1:d9:57:12:15:5f:81:d3:ab:40:66:2a:
  3d:ab:d4:fb:24:a6:dd:1f:82:a2:33:9d:3d:da:a7:75:fa:0d:
  e6:be:1f:3b:a9:7f:d0:94:67:bf:e7:8b:19:32:5c:ea:0f:ae:
  3e:1e:41:55:06:c9:cb:42:b9:45:de:0e:d9:48:a5:75:90:5b:
  d7:89:ff:60:f2:31:ed:d7:52:0a:3d:91:87:c3:9a:85:76:8a:
  44:6f:c5:4e:9b:65:f6:78:cf:ee:7b:28:f5:10:c8:d1:39:3f:
```

```

13:a7:96:f1:4b:11:5f:34:96:8f:13:b1:b6:de:9c:23:9e:f6:
9d:b8:a3:f7:03:07:76:ce:bd:f6:76:1d:fc:5d:83:1e:8e:74:
fb:78:b6:4a:ad:73:ce:e7:71:72:7d:0a:1e:49:5d:9e:65:30:
aa:6f:b4:2f:9d:c3:e5:e6:38:de:0b:26:20:69:98:e4:6d:99:
d2:15:ec:bd

```

Output Fields of the **show web-server status** command

Field	Description
Source	Certificate source: <ul style="list-style-type: none"> <li>● Default: default self-signed certificate</li> <li>● Installed: installed certificate</li> </ul>
Certificate	Certificate information.

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.5 show web-server status

Use this command to display the configuration and status of the Web service.

**show web-server status**

#### Parameter Description

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration and status of the Web service:

```

Hostname#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http redirect to https: false

```

Output Fields of the **show web-server status** command

Field	Description
http server status	HTTP server status
http server port	HTTP server port
https server status	HTTPS server status
https server port	HTTPS server port
http redirect to https	Whether to enable HTTP-to-HTTPS

#### Related Commands

Command	Description
<b>enable service web-server</b>	Enables the HTTP service.
<b>http port</b>	Configures the HTTP port number.
<b>http secure-port</b>	Configures the HTTPS port number.

**Platform** N/A

#### Description

## 1.6 webmaster level

Use this command to configure the username and password for Web login authentication. Use the **no** form of this command to restore the default setting.

**webmaster level** *privilege-level* **username** *name* **password** { *password* | [ **0** | **7** ] *encrypted-password* }

**no webmaster level** *privilege-level* [ **username** *name* ]

#### Parameter Description



Parameter	Description
<i>privilege-level</i>	Configures the user privilege level.
<i>name</i>	Username.
<i>password</i>	Password.
<b>0</b>   <b>7</b>	Password type. The value 0 indicates cleartext and the value 7 indicates ciphertext.
<i>encrypted-password</i>	Password text.

**Defaults** User is configured with privilege level 0, username of admin and plaintext password of admin.

**Command mode** Global configuration mode.

**Usage Guide** When HTTP is enabled, users can log in to the Web interface only after being authenticated. Use this command to configure the username and password for Web login authentication. Use the **no webmaster level** *privilege-level* command to delete all the usernames and passwords with a specified *privilege-level*.

Use the **no webmaster level *privilege-level* username *name*** command to delete the specified username and password.

-  Usernames and passwords come with three permission levels, each of which includes at most 10 usernames and passwords.
-  The system creates account **admin** by default. The account cannot be deleted and only its password can be changed. The administrator account **admin** corresponds to the level 0 privilege. Account **admin** owns all the function privileges on the Web client and can edit other management accounts and authorize the accounts to access pages. New accounts correspond to the level 1 privilege.

**Configuration Examples** The following example sets the privilege level bound to a user for logging in to the Web page to **0**, username to **Hostname**, and password to **admin**.

```
Hostname(config)# webmaster level 0 username Hostname password admin
```

**Notifications** When the default account **admin** is deleted, the following notification will be displayed.

```
%notice: Cannot cancel the default user configure!
```

When the number of configured usernames exceeds 10 at each permission level, the following notification will be displayed.

```
%notice: configure webmaster level %d server reached max 10, add failed.
```

When the configured username reaches or exceeds 32 characters, the following notification will be displayed.

```
%notice: Username too long. Please enter less than 32 characters.
```

If the configured password length is fewer than 8 or contains only letters or numerals, the following notification will be displayed

```
User_access warning: the password is too weak, default min-size(8) and should contain two different characters.
```

If the configured password does not meet complexity requirements, the following notification will be displayed

```
User_access reject: invalid password, the password is too simple.
```

If the configured password is the same as the username, the following notification will be displayed.

```
% Password should not be the same as username.
```

**Related Commands**

Command	Description
<b>enable service web-server</b>	Enables the HTTP service.

**Platform** N/A  
**Description**

## 1.7 web-server http redirect-to-https

Use this command to configure automatic HTTP redirection to HTTPS.

**web-server http redirect-to-https**

Run the **no** form of this command to restore the default configuration.

**no web-server http redirect-to-https**



Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Automatic HTTP redirection to HTTPS is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** When a user uses a browser to access the Web management system through HTTP upon configuration of HTTP redirection to HTTPS, the Web server address automatically redirects to HTTPS.

The **no web-server http redirect-to-https** or **default web-server http redirect-to-https** command is used to disable automatic HTTP redirection to HTTPS.

-  HTTP automatically redirects to HTTPS only when the HTTP and HTTPS services are enabled.
-  If an IP address to be accessed is a Network Address Port Translation (NAPT) address, the redirection function may fail. In this case, to access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

**Configuration Examples** The following example configures HTTP redirection to HTTPS when a user accesses the Web page through HTTP :

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server http redirect-to-https
    
```

**Verification** Use the **show web-server status** command to display the status of the Web service.

**Notifications** The following example configures HTTP redirection to HTTPS when a user accesses the Web page through HTTP :

```

%notice: available unless https is enabled.
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.8 web-server https certificate

Run this command to install an HTTPS certificate

```
web-server https certificate { pem cert-filename private-key key-filename } | { pfx cert-filename }
[ password password-text ]
```

Run the **no** form of this command to restore the default configuration.

```
no web-server https certificate
```

### Parameter Description

Parameter	Description
<b>pem</b>	Imports the certificate file and private key file in the pem format.
<b>pfx</b>	Imports the certificate file in the pfx format from which a private key is exported.
<i>cert-filename</i>	Name of the certificate file under the <b>flash:</b> drive.
<i>key-filename</i>	Name of the private key file under the <b>flash:</b> drive.
<i>password-text</i>	Decryption password of the private key file or decryption password of the private key exported from the pfx certificate.

### Defaults

N/A

### Command mode


Global configuration mode

### Usage Guide

Run the **copy** command to copy the certificate/private key file to the **flash:** partition before running the **web-server https certificate** command to install the HTTPS service certificate. After installation, you can delete the certificate/private key file from the **flash:** partition.

You can run the **no web-server https certificate** command to remove the installed HTTPS service certificate. After deletion, the HTTPS service will use the self-signed certificate.

 This command is not displayed in the configuration.

 After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

### Configuration Examples

The following example configures the device to install the HTTP certificate: Install the certificate file **usercert.pfx** under the **flash:** partition. The password for exporting the certificate file is 123456:

```
Hostname# configure terminal
Hostname(config)# web-server https certificate pfx usercert.pfx password
123456
*Feb 28 14:38:37: %HTTPD-4-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```



**Verification** Use the **show web-server https certificate information** command to display information about the HTTPS service certificate.

**Notifications** When the certificate is installed, the following notification will be displayed:  
 % The certificate was successfully installed.  
 When the size of the file name exceeds 64 bytes, the following notification will be displayed:  
 % Operation failed: filename too long, should be less than 64 bytes.  
 When the certificate fails to match the private key file, the following notification will be displayed:  
 % Operation failed: certificate does not matched with private key.  
 When the certificate file does not exist or is empty, the following notification will be displayed:  
 % Operation failed: certificate file not found or is empty.  
 When the private key file does not exist or is empty, the following notification will be displayed:  
 % Operation failed: private key file not found or is empty.  
 When the password is incorrect, the following notification will be displayed:  
 % Operation failed: please input correct password.  
 When an error is reported during parsing of the certificate file or private key file, the following notification will be displayed:  
 % Operation failed: verify file failed.  
 When the certificate is not installed but the certificate deletion command is run, the following notification will be displayed:  
 % Operation failed: no certificate installed.  
 When the certificate is deleted, the following notification will be displayed:  
 % The installed certificate was successfully deleted.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 web-server https generate self-signed-certificate

Run this command to generate an HTTPS service self-signed certificate again.  
**web-server https generate self-signed-certificate**


Parameter Description	Parameter	Description
	N/A	N/A


**Defaults** The HTTPS service uses the self-signed certificate by default.

**Command mode** Global configuration mode

**Usage Guide** This command is an interactive command. After running this command, enter the information to generate a self-signed certificate as prompted including the number of RSA key modulus digits and certificate username, or press **Ctrl+C** to cancel the operation.

If the device is installed with a third-party HTTPS service certificate, the device uses the HTTPS certificate preferentially. The re-generated self-signed certificate does not replace the current HTTPS service certificate.

 When the **show running-config** command is run, this command is not displayed.

 After the HTTPS service certificate is generated again, the browser may require you add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

**Configuration** The following example generates an HTTPS service self-signed certificate again.

**Examples**

```

Hostname# configure terminal
Hostname(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully.
    
```

**Verification** Use the **show web-server https certificate information** command to display information about the HTTPS service certificate.

**Notifications** When the modulus length of the entered RSA key is not in the range from 1024 to 4096 or is not a number, the following notification will be displayed:

```
% Invalid number.
```

If you press **Ctrl+C** when an input prompt is displayed, the operation will be canceled and the following notification will be displayed:

```
% Operation cancelled.
```

When the length of the entered certificate username exceeds 64 bytes, the following notification will be displayed:

```
% Input too long, should not exceed 64 bytes.
```

When a self-signed certificate is generated, the following notification will be displayed:

```
% Generate self-signed certificate successfully.
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

# 1 Syslog Commands

## 1.1 clear logging

Use this command to clear the logs from the buffer in privileged EXEC mode.

### clear logging

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.

Configuration The following example clears the log packets from the memory buffer.

Examples 

```
Hostname# clear logging
```

Related Commands	Command	Function
	<b>logging on</b>	Enables the log function.
	<b>show logging</b>	Displays the logs in the buffer.
	<b>logging buffered</b>	Records the logs in the memory buffer.

Platform Description N/A

## 1.2 logging

Use this command to send the log message to the specified syslog server.

**logging** { *ip-address* | **IPv6** *IPv6-address* } [ **udp-port** *port* ]

Use this command to delete the specified syslog server.

**no logging** { *ip-address* ] | **IPv6** *IPv6-address* }

Use this command to restore the default port 514.

**no logging** { *ip-address*] | **IPv6** *IPv6-address* } **udp-port**

Parameter	Parameter	Description
Description		

<i>ip-address</i>	<b>Sets</b> the IP address of the host receiving log messages.
<i>IPv6-address</i>	Sets the IPv6 address of the host receiving log messages.
<b>udp-port</b> <i>port</i>	Sets the port number of the host receiving log messages. The default is 514.

**Defaults** No log message is sent to syslog server by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously.

**Configuration Examples** The following example configures a syslog server with IP address 202.101.11.1.

```
Hostname(config)# logging 202.101.11.1
```

The following example configures a syslog server with IP address 10.1.1.100 and port number 8099.

```
Hostname(config)# logging 202.101.11.1 udp-port 8099
```

The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF.

```
Hostname(config)# logging IPv6 AAAA:BBBB::FFFF
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.3 logging buffered

Use this command to set the memory buffer parameters (log severity and buffer size) for logs at global configuration layer. Use the **no** form of the command to disable recording logs in the memory buffer.

Use the **default** form of this command to restore the default setting.

**logging buffered** [ *buffer-size* | *level* ]

**no logging buffered**

**default logging buffered**

Parameter Description	Parameter	Description
	<i>buffer-size</i>	The value ranges from 4 Kbytes to 128 Kbytes.
	<i>level</i>	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.

**Defaults** The buffer size is 4 K Bytes

The log severity is 7.

**Command**

**Mode** Global configuration mode

**Usage Guide**

The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the **show logging** command in privileged user mode.


The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the **clear logging** command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server.

The log information is classified into the following 8 levels (Table 1):

**Table-1**

Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level. When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.

 After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficient available continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.

**Configuration**

The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes.

**Examples**

```
Hostname(config)# logging buffered 10000 6
```

**Related**

**Commands**

Command	Description
<b>logging on</b>	Turns on the log switch.
<b>show logging</b>	Displays the logs in the buffer.
<b>clear logging</b>	Clears the logs in the log buffer.

**Platform**  
**Description** N/A

## 1.4 logging console

Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the **no** form of this command to prohibit printing log messages on the console.

**logging console** [ *level* ]

**no logging console**

Parameter	Parameter	Description
<b>Description</b>	<i>level</i>	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** When a log severity is set, the log messages at or below that severity will be displayed on the console.  
The **show logging** command displays the related setting parameters and statistics of the log.

**Configuration Examples** The following example sets the severity of log that is allowed to be displayed on the console as 6:

```
Hostname(config)# logging console informational
```

Related Commands	Command	Description
	<b>logging on</b>	Turns on the log switch.
	<b>show logging</b>	Displays the logs and related log configuration parameters in the buffer.

**Platform**  
**Description** N/A

## 1.5 logging count

Use this command to enable the log statistics function in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging count**

**no logging count**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The log statistics function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command enables the log statistics function. The statistics begins when the function is enabled. If you run the **no logging count** command, the statistics function is disabled and the statistics data is deleted.

**Configuration** The following example enables the log statistics function:

**Examples** `Hostname(config)# logging count`

Related Commands	Command	Description
	<b>show logging count</b>	Displays log information about modules of the system.
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.

**Platform Description** N/A

## 1.6 logging delay-send file

Use this command to set the name of the log file saved locally for delay sending. Use the no form of this command to restore the default setting.

**logging delay-send file flash:filename**

**no logging delay-send file**

Parameter	Parameter	Description
Description	<b>flash:filename</b>	Sets the name of the log file saved locally for delay sending.

**Defaults** The default name format is as follows: file size\_device IP address\_index.txt. If you want to change the file name, the file sent to the remote server should be named as follows: prefix\_ file size\_device IP address\_index.txt; the file saved locally should be named as follows: prefix\_index.txt. The default prefix is syslog\_ftp\_server.

**Command** Global configuration mode  
**Mode**

**Usage Guide** The file name cannot contain special symbols including . \ : \* " < > and |.  
 For example, the file name is log\_server, file index 5, file size 1000B and device IP address 10.2.3.5. The log file sent to the remote server is named log\_server\_1000\_10.2.3.5\_5.txt and the log file saved locally is named log\_server\_5.txt.  
 If the device has an IPv6 address, the colon (:) in the IPv6 address is replaced by the hyphen (-). For example, the is log\_server, file index 6, file size 1000B and device IPv6 address 2001::1. The log file sent to the remote server is named log\_server\_1000\_2001-1\_6.txt and the log file saved locally is named log\_server\_6.txt.

**Configuration** The following example sets the name of the log file saved locally to log\_server.

**Examples**

```
Hostname(config)# logging delay-send file flash:log_server
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.7 logging delay-send interval

Use this command to set the interval at which log sending is delayed. Use the no form of this command to restore the default setting.

**logging delay-send interval seconds**

**no logging delay-send interval**

**Parameter  
Description**

Parameter	Description
seconds	Sets the interval at which log sending is delayed, in the range from 600 to 65535 seconds.

**Defaults** The default is 3600.

**Command  
Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the the interval at which log sending is delayed to 600 seconds.

**Examples**

```
Hostname(config)# logging delay-send interval 600
```



<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.8 logging delay-send server

Use this command to configure the server address and log sending mode. Use the no form of this command to restore the default setting.

**logging delay-send server** { *ip-address* | **IPv6** *IPv6-address* } **mode** { **ftp user** *username* **password** [ **0** | **7** ] *password* | **tftp** }

**no logging delay-send server** { *ip-address* | **IPv6** *IPv6-address* }

<b>Parameter Description</b>	Parameter	Description
	<i>ip-address</i>	Specifies the IP address of the server.
	<b>IPv6</b> <i>IPv6-address</i>	Specifies the IPv6 address of the server.
	<i>username</i>	Sets the FTP server username.
	<i>password</i>	Sets the FTP server password.
	<b>0</b>	(Optional) The password is displayed in plaintext.
<b>7</b>	The password are encrypted.	

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to specify an FTP/TFTP server to receive logs. You can configure five FTP/TFTP servers. Logs are sent to all configured servers simultaneously.

**Configuration Examples** The following example specifies an FTP server whose IP address is 192.168.23.12, username admin and password admin.

```
Hostname(config)# logging delay-send server 192.168.23.12 mode ftp user
admin password admin
```

The following example specifies a TFTP server whose IPv6 address is 2000::1.

```
Hostname(config)# logging delay-send server IPv6 2000::1 mode tftp
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform**  
**Description** N/A

## 1.9 logging delay-send terminal

Use this command to enable delay in sending logs to console and remote terminal. Use the no form of this command to restore the default setting.

**logging delay-send terminal**  
**no logging delay-send terminal**

<b>Parameter</b> <b>Description</b>	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example enables delay in sending logs to console and remote terminal.

**Examples**

```
Hostname(config)# logging delay-send terminal
```

<b>Related</b> <b>Commands</b>	Command	Description
	N/A	N/A

**Platform**  
**Description** N/A

## 1.10 logging facility

Use this command to configure the device value of the log information in global configuration mode. Use the **no** form of the command to restore the default setting.

**logging facility facility-type**  
**no logging facility**

<b>Parameter</b> <b>Description</b>	Parameter	Description
	<i>facility-type</i>	Syslog device value. For specific settings, refer to the usage guide.

**Defaults** The default is 23 if the RFC5424 format is enabled (Local7, local use).  
The default is 16 if the RFC5424 format is disabled (Local0, local use).

**Command Mode** Global configuration mode

**Usage Guide** The following table (Table-2) is the possible device values of Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization messages
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer subsystem
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization messages
11 (ftp)	FTP daemon
12 (ntp)	NTP subsystem
13 (logaudit)	log audit
14 (logalert)	log alert
15 (clock2)	clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value of RGOS is 23 (local 7).

**Configuration** The following example sets the device value of **Syslog** as **kernel**:

**Examples** `Hostname(config)# logging facility kern`

Related Commands	Command	Description
	<b>logging console</b>	Sets the severity of logs that are allowed to be displayed on the console.

**Platform Description** N/A

## 1.11 logging file

Run the **logging file** command to save logs to files. Log files can be stored in the hard disk, extended flash space, USB flash drive, or SD card. Use the no form of this command to restore the default setting,

**logging file** { **sata0:filename** | **flash:filename** | **usb0:filename** | **usb1:filename** | **sd0:filename** }  
 [ *max-file-size* ] [ *level* ]

**no logging file**

Parameter Description	Parameter	Description
	<b>sata0</b>	Saves the log file in hardware disk.
	<b>flash</b>	Saves the log file in expanded FLASH (when there is flash2, the log files will be saved to flash2).
	<b>usb0</b>	Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device.
	<b>usb1</b>	Saves the log file in USB1, This parameter is supported by the device with two USB connectors and the USB extension device.
	<b>sd0</b>	Saves the log file in the SD card. This parameter is supported by the device with the SD card interface and the SD card extension device.
	<i>filename</i>	Sets the file name. The file type is omitted, which is fixed as txt.
	<i>max-file-size</i>	Sets the maximum file size, in the range from 128K to 6M bytes, The default is 128K,
	<i>level</i>	Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details.

**Defaults** Log messages are not saved in expanded FLASH by default.

**Command Mode** Global configuration mode

**Usage Guide** You can save log messages in expanded FLASH if you don't want to transmit log messages on the network or there is no syslog server,  
 The log file cannot be configured with the suffix, which is fixed as txt.

**i** If there is no expanded FLASH, the **logging file flash** command is hidden automatically and cannot be configured.

Keyword	Level	Description
Emergencies	0	Emergency case. The system fails to run.
Alerts	1	Problem that call for immediate solution.
Critical	2	Critical message.
Errors	3	Error message.
warnings	4	Alarm message.
Notifications	5	message that is normal but calls for attention.
informational	6	Descriptive message.
Debugging	7	Debugging message

**Configuration Examples** The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively.

```
Hostname(config)# logging file flash:syslog
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.12 logging file numbers

Run the **logging file numbers** command to configure the number of system log files that are written into the extended flash space.

**logging file numbers** *numbers*

Run the **no** form of this command to remove this configuration and restore the default configuration.  
**no logging file numbers**

**Parameter Description**

Parameter	Description
<i>numbers</i>	Number of log files. The value range is from 2 to 16.

**Defaults** The default is 16.

**Command** Global configuration mode  
**Mode**

**Usage Guide** You can use the **logging file numbers** command to set the number of log files, and run the **no** form of this command to restore the default number of log files to 16.

The system will not delete the generated log files after the number of log files is modified. Therefore, to save the extended flash space, you need to manually delete the log files generated in the system (before deletion, you can transfer the log files to an external server through TFTP). For example, 16 log files will be created by default after the function of writing logs into log files is enabled. If the device has generated 16 log files and if you want to change the number of log files to 2, new logs are overridden or overwritten in the log files with the index of 0 and 1 by turns. The existing log files with the index of 2 to 16 are retained. You can manually delete them.

**Configuration** The following example sets the number of log files to 8.

**Examples**

```
Hostname(config)# logging file numbers 8
```

**Verification** Run the **show run** command to display the number of log files.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.13 logging flash flush

Use this command to write log messages in the system buffer into the flash file immediately.

**logging flash flush**


**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command** Global configuration mode  
**Mode**

**Usage Guide** In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.

 The **logging flash flush** command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.

**Configuration** The following example writes log messages in the system buffer into the flash file immediately.

**Examples** `Hostname(config)# logging flash flush`

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.14 logging flash interval

Use this command to set the interval to write log messages into the flash file, Use the no form of this command to restore the default setting.


**logging flash interval** *seconds*  
**no logging flash interval**

<b>Parameter Description</b>	Parameter	Description
	<b>interval</b> <i>seconds</i>	The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds.

**Defaults** The default is 3600.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the no logging flash interval command.

 To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.

**Configuration** The following example sets the interval to write log messages into the flash file to 300 seconds.

**Examples** `Hostname(config)# logging flash interval 300`

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.15 logging filter direction

Use this command to filter the log messages destined to a certain direction. Use the no form of this command to restore the default setting.

**logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

**no logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

Parameter Description	Parameter	Description
	<b>all</b>	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
	<b>buffer</b>	Log messages destined to the log buffer are filtered, including log messages displayed by running the show logging command.
	<b>file</b>	Log messages destined to the log file are filtered.
	<b>server</b>	Log messages destined to the log server are filtered.
	<b>terminal</b>	Log messages destined to the console and the VTY terminal (including Telnet and SSH).

**Defaults** Log messages destined to all directions are filtered by default.

**Command Mode** Global configuration mode

**Usage Guide** In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the terminal parameter.

**Configuration Examples** The following example filters log messages destined to the terminal (including the console and the VTY terminal).

```
Hostname(config)# logging filter direction terminal
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**



## 1.16 logging filter type

Use this command to configure the filter type of log messages. Use the no form of this command to restore the default setting.

**logging filter type { contains-only | filter-only }**



**no logging filter type**

Parameter Description	Parameter	Description
	<b>contains-only</b>	The log message containing the key word of the filter rule is printed.
	<b>filter-only</b>	The log message containing the key word of the filter rule is filtered.

**Defaults** The default filter type is filter-only.

**Command Mode** Global configuration mode

**Usage Guide** When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the “filter-only” filter type to filter the log messages, If you are concerned with certain log messages, use the “contains-only” filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.

-  In real operation, the contains-only and the filter-only filter types cannot be configured at the same time.
-  If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.

**Configuration Examples** The following example sets the filter type to contains-only.

```
Hostname(config)# logging filter type contains-only
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.17 logging filter rule

Use this command to configure the filter rule of the log message,

**logging filter rule { exact-match module *module-name* mnemonic *mnemonic-name* level *level* | single-match [ level *level* | mnemonic *mnemonic-name* | module *module-name* ] }**

Use this command to delete the “exact-match” filter rule.

**no logging filter rule exact-match** [ **module** *module-name* **mnemonic** *mnemonic-name* **level** *level* ]

Use this command to delete the “single-match” filter rule.

**no logging filter rule single-match** [ **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* ]

Parameter Description	Parameter	Description
	<b>exact-match</b>	Exact-match filter rule. Fill in all the following three parameters.
	<b>single-match</b>	Single-match filter rule. Fill in one of the following three parameters.
	<b>module</b> <i>module-name</i>	Module name.
	<b>mnemonic</b> <i>mnemonic-name</i>	Mnemonic name.
	<b>level</b> <i>level</i>	Log level,

**Defaults** No filter rule is configured by default,

**Command Mode** Global configuration mode

**Usage Guide** If you want to filter a specific log message, use the “exact-match” filter rule and fill in all three parameters, namely, module name, mnemonic name and log level.  
 If you want to filter a specific kind of log messages, use the “single-match” filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level.  
 When configured with the same module name, mnemonic name or log level, the “single-match” filter rule has a higher priority than the “exact-match” filter rule,

**Configuration Examples** The following example configures the “exact-match” filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT.

```
Hostname(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

The following example configures the “single-match” filter rule with the parameter of module name SYS.

```
Hostname(config)# logging filter rule single-match module SYS
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.18 logging life-time

Use this command to configure the preservation duration of logs in expanded FLASH. Use the **no** form of this command to restore the default setting.

**logging life-time level** *level days*

**no logging life-time level** *level*


### Parameter Description

Parameter	Description
<i>level</i>	Sets the log level, which can be either the level name or the level number.
<i>days</i>	Sets the preservation duration of logs.

**Defaults** No preservation duration is set by default.

**Command Mode** Global configuration mode

**Usage Guide** Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.

 Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the `syslog/` directory of the expanded FLASH,

**Configuration Examples** The following example sets the preservation duration of logs whose level is 6 to 10 days.

```
Hostname(config)# logging life-time level 6 10
```

### Related Commands

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.19 logging monitor

Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the **no** form of this command to disable this function.

**logging monitor** [*level*]

**no logging monitor**

Parameter	Description
-----------	-------------

<b>Parameter Description</b>	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.
------------------------------	--------------	---

**Defaults** The default is debugging (7).

**Command Mode** Global configuration mode

**Usage Guide** To print log information on the VTY window, run the **terminal monitor** command in privileged EXEC mode. The level of logs to be displayed is defined by **logging monitor**.  
The log level defined with "Logging monitor" is for all VTY windows.

**Configuration Examples** The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

```
Hostname(config)# logging monitor informational
```

Related Commands	Command	Description
	<b>logging on</b>	Turns on the log switch.
	<b>show logging</b>	Displays the log messages and related log configuration parameters in the buffer.

**Platform Description** N/A

## 1.20 logging on

Use this command globally to allow logs to be displayed on different devices. Use the **no** form of this command to disable this function.

**logging on**

**no logging on**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Logs are allowed to be displayed on different devices.

**Command Mode** Global configuration mode

**Usage Guide** Log information can not only be shown in the Console window and VTY window, but also be recorded in different devices such as the memory buffer, the expanded FLASH and the Syslog

Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is less than 1.

**Configuration** The following example disables the log switch on the device.

**Examples** `Hostname(config)# no logging on`

Related Commands	Command	Description
	<b>logging buffered</b>	Records the logs to a memory buffer.
	<b>logging server</b>	Sends logs to the Syslog server.
	<b>logging file flash:</b>	Records logs on the expanded FLASH.
	<b>logging console</b>	Allows the log level to be displayed on the console.
	<b>logging monitor</b>	Allows the log level to be displayed on the VTY window (such as telnet window) .
	<b>logging trap</b>	Sets the log level to be sent to the Syslog server.

**Platform** N/A  
**Description**

## 1.21 logging policy

Use this command to configure the severity ranking policy. Use the no form of this command to remove one policy, Use the no logging policy command to remove all policies.

**logging policy module** *module-name* [ **not-lesser-than** ] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

**no logging policy module** *module-name* [ **not-lesser-than** ] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

**no logging policy**

Parameter Description	Parameter	Description
	<i>module-name</i>	The name of the module applying the ranking policy.
	<b>not-lesser-than</b>	If this parameter is specified, only when the log's level is not lower than the configured level can the log be sent. Otherwise, the log is filtered. If this parameter is not specified, only when the log's level is not higher than the configured level can the log be sent. Otherwise, the log is filtered.
	<i>level</i>	Severity level
	<b>all</b>	Applies the ranking policy in all directions.
	<b>server</b>	Applies the ranking policy to the direction toward the server.
	<b>file</b>	Applies the ranking policy to the direction toward the log file.
	<b>console</b>	Applies the ranking policy to the direction toward the console.
	<b>monitor</b>	Applies the ranking policy to the direction toward the remote server.

<b>buffer</b>	Applies the ranking policy to the direction toward the buffer.
---------------	--

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to send logs to different destinations based on module and severity.

**Configuration Examples** The following example sends logs of the SYS module leveled above 5 to the console and sends logs of the SYS module leveled below 3 to the buffer.

```

Hostname(config)# logging policy module SYS not-lesser-than 5 direction
console
Hostname(config)# logging policy module SYS 3 direction buffer
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.22 logging rate-limit

Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the **no** form of this command to disable this function.

**logging rate-limit** { *number* | **all** *number* | **console** { *number* | **all** *number* } } [ **except** *severity* ]

**no logging rate-limit**

Parameter Description	Parameter	Description
	<i>number</i>	The number of logs that can be processed in a second in the range from 1 to 10000.
	<b>all</b>	Sets rate limit to all the logs with severity level 0 to 7.
	<b>console</b>	Sets the amount of logs that can be shown in the console in a second.
	<b>except</b>	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
	<i>severity</i>	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.

**Defaults** The log rate limit function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to control the syslog output to prevent the massive log output.

**Configuration Examples** The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled:

```
Hostname(config)#logging rate-limit all 10 except warnings
```

Related Commands	Command	Description
	<b>show logging count</b>	Displays log information about modules of the system.
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.

**Platform Description** N/A

## 1.23 logging server

Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

**logging server** { *ip-address* | **IPv6** *IPv6-address* } [ **udp-prot** *port* ]

**no logging server**{ *ip-address* | **IPv6** *IPv6-address* }

**no logging server** { *ip-address* | **IPv6** *IPv6-address* } **udp-prot**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the IP address of the host that receives log information.
	<i>IPv6-address</i>	Specifies the IPv6 address for the host receiving the logs.
	<i>port</i>	Specifies the port number for the specified host (The default port number is 514).

**Defaults** No log is sent to any syslog server by default.

**Command Mode** Global configuration mode

**Usage Guide** This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time.

**Configuration** The following example specifies a syslog server of the address 202.101.11.1:

**Examples** `Hostname(config)# logging server 202.101.11.1`

The following example specifies a syslog server with IP address 10.1.1.100 and port 8099.

`Hostname(config)# logging server 202.101.11.1 udp-port 8099`

The following example specifies an ipv6 address as AAAA:BBBB:FFFF:

`Hostname(config)# logging server IPv6 AAAA:BBBB:FFFF`

Related Commands	Command	Description
	<code>logging on</code>	Turns on the log switch.
	<code>show logging</code>	Displays log messages and related log configuration parameters in the buffer.
	<code>logging trap</code>	Sets the level of logs allowed to be sent to Syslog server.

**Platform Description** N/A

## 1.24 logging source interface

Use this command to configure the source interface of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging source interface** *interface-type interface-number*

**no logging source interface**

Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

**Defaults** No source interface is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.

**Configuration** The following example specifies loopback 0 as the source address of the syslog messages:

**Examples** `Hostname(config)# logging source interface loopback 0`



Related	Command	Description
Commands	<b>logging server</b>	Sends logs to the Syslog server.

**Platform**  
**Description** N/A

## 1.25 logging source ip | IPv6

Use this command to configure the source IP address of logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**logging source** { **ip** *ip-address* | **IPv6** *IPv6-address* }

**no logging source** { **ip** | **IPv6** }

Parameter	Parameter	Description
<b>Description</b>	<i>ip-address</i>	Specifies the source IPV4 address sending the logs to IPV4 log server.
	<i>IPv6-address</i>	Specifies the source IPV6 address sending the logs to IPV6 log server.

**Defaults** No source address is configured by default.

**Command**  
**Mode** Global configuration mode

**Usage Guide** By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.

**Configuration** The following example specifies 192.168.1.1 as the source address of the syslog messages:

**Examples**

```
Hostname(config)# logging source ip 192.168.1.1
```

Related	Command	Description
Commands	<b>logging server</b>	Sends the logs to the Syslog server.

**Platform**  
**Description** N/A

## 1.26 logging statistic enable

Use this command to enable logging periodically. Use no form of this command to restore the default setting.

**logging statistic enable**

**no logging statistic enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to send performance statistics at a certain interval for the server to monitor the system performance.

**Configuration Examples** The following example enables logging periodically.

```
Hostname(config)# logging statistic enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.27 logging statistic mnemonic

Use this command to configure the interval at which logs are sent. Use the no form of this command to restore the default setting.

**logging statistic mnemonic *mnemonic interval minutes***

**no logging statistic mnemonic *mnemonic***

Parameter Description	Parameter	Description
	<i>mnemonic</i>	Sets the mnemonics to identify the object.
	<i>minutes</i>	Sets the interval at which logs are sent, in the unit of minutes.

**Defaults** The default is 15.

**Command** Global configuration mode  
**Mode**

**Usage Guide** The available settings include 0, 15, 30, 60 and 120. 0 indicates this function is disabled.

**Configuration** The following example set the interval at which logs are sent to 30 minutes.

**Examples** `Hostname(config)# logging statistic mnemonic TUNNEL_STAT interval 30`

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.28 logging statistic terminal

Use this command to enable logs to be sent to the console and the remote terminal periodically. Use the no form of this command to restore the default setting.

**logging statistic terminal**  
**no logging statistic terminal**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example enable logs to be sent to the console and the remote terminal.

**Examples** `Hostname(config)# logging statistic terminal`

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.29 logging synchronous

Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the **no** form of this command to restore the default setting.

**logging synchronous**

**no logging synchronous**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The synchronization function between user input and log output is disabled by default.

**Command Mode** Line configuration mode

**Usage Guide** This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters.

**Configuration** Hostname(config)#**line console 0**

**Examples** Hostname(config-line)#**logging synchronous**

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```

Hostname# configure terminal
Oct 9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed
state to down
Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet 0/1, changed state to DOWN
Hostname# configure terminal//----the input command by the user is
output again rather than being intererupted.

```

Related	Command	Description
Commands	<b>show running-config</b>	Displays the configuration.

**Platform Description** N/A

## 1.30 logging trap

Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the **no** form of this command to prohibit sending log messages to the Syslog server.

**logging trap** [*level*]

**no logging trap**

Parameter	Parameter	Description
Description	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.

**Defaults** The default is informational(6)

**Command Mode** Global configuration mode

**Usage Guide** To send logs to the Syslog Server, run the **logging** command in global configuration mode to configure the **Syslog Server**. Then, run the **logging trap** command to specify the severity level of logs to be sent.  
The **show logging** command displays the configured related parameters and statistics of the log.

**Configuration Examples** The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

```

Hostname(config)# logging 202.101.11.22
Hostname(config)# logging trap informational
    
```

Related Commands	Command	Description
	<b>logging on</b>	Turns on the log switch.
	<b>logging</b>	Sends logs to the Syslog server.
	<b>show logging</b>	Displays the log messages and related log configuration parameters in the buffer.

**Platform Description** N/A

### 1.31 logging userinfo

Use this command to enable the logging function to record user log/exit. Use the no form of this command to restore the default setting.

**logging userinfo**

**no logging userinfo**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** Log message is printed recording user log/exit by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows:

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0
(192.168.23.68) OK.
```

**Configuration Examples** The following example enables the logging function to record user log/exit.

```
Hostname(config)# logging user-info
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.32 logging userinfo command-log

Use this command to enable the logging function to record user operation. Use the no form of this command to restore the default setting.

**logging userinfo command-log**

**no logging userinfo command-log**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** Log message is printed recording user operation by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68)
command-log: logging server 192.168.23.68.
```

**Configuration Examples** The following example enables the logging function to record user operation.

```
Hostname(config)# logging user-info command-log
```

Related Commands	Command	Description
		N/A

**Platform** N/A  
**Description**

### 1.33 service log-format rfc5424

Use this command to enable the RFC5424 format. Use the no form of this command to restore the default setting.

**service log-format rfc5424**

**no service log-format rfc5424**

Parameter Description	Parameter	Description
		N/A

**Defaults** The RFC3164 format is used by default.

**Command Mode** Global configuration mode

**Usage Guide** After the RFC5424 format is enabled, the service sequence-numbers, service sysname, **service timestamps**, **service private-syslog** and **service standard-syslog** commands become invalid and hidden.

After switching back to the RFC3164 format, the **logging delay-send**, **logging policy** and **logging statistic** commands become invalid and hidden.

After switching the log format, the results of running the **show logging** and **show logging config** commands change,

**Configuration** The following example enables the RFC5424 format.

**Examples**

```
Hostname(config)# service log-format rfc5424
```

Related Commands	Command	Description
		N/A

**Platform** N/A  
**Description**

## 1.34 service private-syslog

Use this command to set the syslog format to the private syslog format. Use the `no` form of this command to restore the default setting.

**service private-syslog**

**no service private-syslog**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The syslog is displayed in the default format.

**Command Mode** Global configuration mode

**Usage Guide** By default, the syslog is displayed in the format as follows:

\*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console
```

The difference between the private syslog format and the default syslog format lies in the following marks:

The private syslog does not have "\*" before the timestamp, ":" after the timestamp and "%" before the identifying string.

**Configuration** The following example sets the private syslog format.

**Examples**

```
Hostname(config)# service private-syslog
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.35 service sequence-numbers

Use this command to attach serial numbers into the logs in global configuration mode. Use the `no` form of this command to restore the default setting.



**service sequence-numbers**

**no service sequence-numbers**

	Parameter	Description
Parameter		
Description	N/A	N/A

**Defaults** No serial number is contained in the logs by default.

**Command Mode** Global configuration mode

**Usage Guide** In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.

**Configuration Examples** The following example adds serial numbers to the logs.

```
Hostname(config)# service sequence-numbers
```

	Command	Description
<b>Related Commands</b>	<b>logging on</b>	Turns on the log switch.
	<b>service timestamps</b>	Attaches timestamps to the logs.

**Platform Description** N/A

### 1.36 service standard-syslog

Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the no form of this command to restore the default setting.

**service standard-syslog**

**no service standard-syslog**

	Parameter	Description
Parameter		
Description	N/A	N/A

**Defaults** The syslog is displayed in the default format.

**Command Mode** Global configuration mode

**Usage Guide** By default, the syslog is displayed in the format as follows:  
 \*timestamp: %facility-severity-mnemonic: description

Here is an example:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

With this function enabled, the syslog is displayed in the format as follows:

timestamp %facility-severity-mnemonic: description

Here is an example:

```
May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console
```

The difference between the standard syslog format and the default syslog format lies in the following marks:

The standard syslog does not have "\*" before the timestamp and ":" after the timestamp.

**Configuration** The following example sets the standard syslog format.

**Examples**

```
Hostname(config)# service standard-syslog
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.37 service sysname

Use this command to attach system name to logs in global configuration mode. Use the **no** form of this command to restore the default setting.

**service sysname**

**no service sysname**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** No system name is attached to logs by default.

**Command Mode** Global configuration mode

**Usage Guide** This command allows you to decide whether to add system name in the log information.

**Configuration** The following example adds a system name in the log information:

**Examples**

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#service sysname
```

```

Hostname(config)#end
Hostname#
Mar 22 15:35:57 S3250 Hostname %SYS-5-CONFIG: Configured from console by
console
    
```

Related Commands	Command	Function
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.

**Platform Description** N/A

### 1.38 service timestamps

Use this command to attach timestamp into logs in global configuration mode. Use the **no** form of this command to remove the timestamp from the logs. Use the **default** form of this command to restore the default setting.

**service timestamps** [ *message-type* [ **uptime** | **datetime** [ **msec** | **year** ] ] ]

**no service timestamps** [ *message-type* ]

**default service timestamps** [ *message-type* ]

Parameter Description	Parameter	Description
	<i>message-type</i>	The log type, including <b>Log</b> and <b>Debug</b> . The <b>log</b> type indicates the log information with severity levels of 0 to 6. The <b>debug</b> type indicates that with severity level 7.
	<b>uptime</b>	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41.
	<b>datetime</b>	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
	<b>msec</b>	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
	<b>year</b>	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07

**Defaults** The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.

**Command Mode** Global configuration mode

**Usage Guide** When the **uptime** option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the **datetime** option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.

**Configuration Examples** The following example enables the timestamp for **log** and **debug** information, in format of Datetime, supporting millisecond display.

```

Hostname(config)# service timestamps debug datetime msec
Hostname(config)# service timestamps log datetime msec
Hostname(config)# end
Hostname(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from
console by console
    
```

Related Commands	Command	Description
	<b>logging on</b>	Turns on the log switch.
	<b>service sequence-numbers</b>	Enables serial numbers of logs.

**Platform Description** N/A

## 1. 39 show logging

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.

### show logging

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following command displays the result of the **show logging** command with RFC5424 format disabled.

```

Hostname# show logging
Syslog logging: enabled
    
```

```

Console logging: level debugging, 15495 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 15496 messages logged
Standard format: false
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable
Sysname log messages: enable
Count log messages: enable
Trap logging: level informational, 15242 message lines logged,0 fail
  logging to 202.101.11.22
  logging to 192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015489: *Sep 19 02:46:26: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to down.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet 0/24, changed state to down.
015491: *Sep 19 02:46:28: Hostname %LINK-3-UPDOWN: Interface
FastEthernet 0/24, changed state to up.
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.

```

Log information description:

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.

Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

```

Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current
send index:3, Cycle:10 seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
logging to 192.168.23.89
logging to 2000::1
  Delay-send logging: 2641 message lines logged
logging to 192.168.23.89 by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - - Please config the IP
address for capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip
address for capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - - Please config the IP
address for capwap.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip
address for capwap.
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881
name="" type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD
[USER@4881 name=""] [CMD@4881 task="rl_con" cmd="enable"]

```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically

Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands	Command	Function
	<b>logging on</b>	Turns on the log switch.
	<b>clear logging</b>	Clears the log messages in the buffer.

**Platform Description** N/A

### 1.40 show logging config

Use this command to display log configuration and statistics.

**show logging config**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the outcome of running the **show logging config** command with RFC5424 disabled.

```

Hostname# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
    
```

```
Count log messages: enable
Trap logging: level informational, 15242 message lines logged,0 fail
logging to 202.101.11.22
logging to 192.168.200.112
```

Field	Description
Syslog logging	Whether the logging function is enabled or disabled.
Console logging	The level and statistics of the log message printed on the console.
Monitor logging	The level and statistics of the log message printed on the VTY window.
Buffer logging	The level and statistics of the log message recorded in the memory buffer.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of debugging message.
Timestamp log messages	Timestamp format of log message.
Sequence-number log messages	Whether the sequence number function is enabled or disabled.
Sysname log messages	Adds the system name to the log message.
Count log messages	Log-counting function
Trap logging	The level and statistics of the log message sent to the syslog server.

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
Hostname# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current
send index:3, Cycle:10 seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
logging to 192.168.23.89
logging to 2000::1
  Delay-send logging: 2641 message lines logged
logging to 192.168.23.89 by tftp
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics



Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to output console and remove terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending way and statistics

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.41 show logging count

Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.

**show logging count**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** To use the log packet statistics function, run the **logging count** command in global configuration mode. The **show logging count** command can show the information of a specific log, occurrence times, and the last occurrence time.  
 You can use the **show logging** command to check whether the log statistics function is enabled.

**Configuration Examples** The following example displays the result of the **show logging count** command:

```

Hostname# show logging count
Module Name  Message Name Sev  Occur    Last Time
SYS          CONFIG_I      5   1       Jul 6 10:29:57
SYS TOTAL                    1
    
```

Related Commands	Command	Function
	<b>logging count</b>	Enables the log statistics function.
	<b>show logging</b>	Displays basic configuration of log modules and log information in the buffer.
	<b>clear logging</b>	Clears the logs in the buffer.

**Platform Description** N/A

## 1.42 show logging reverse

Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.

**show logging reverse**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the log parameter configurations and log statistics as well as the log packets in the memory buffer. Log messages are displayed based on the timestamp from latest to earliest.

**Configuration Examples** The following command displays the result of the **show logging reverse** command with RFC5424 format disabled.

```

Hostname# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable

```

```

Trap logging: level informational, 15242 message lines logged,0 fail
logging to 202.101.11.22
logging to 192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015491: *Sep 19 02:46:28: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
015490: *Sep 19 02:46:26: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to down.
015488: *Sep 19 02:46:13: Hostname %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Hostname %LINK-3-UPDOWN: Interface FastEthernet
0/24, changed state to up.
    
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

```

Hostname# show logging reverse
Syslog logging: enabled
Console logging: level debugging, 4740 messages logged
    
```

```

Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 4745 messages logged
Statistic log messages: disable
Statistic log messages to terminal: disable
Delay-send file name:syslog_ftp_server, Current write index:3, Current
send index:3, Cycle:10 seconds
Count log messages: enable
Trap logging: level informational, 2641 message lines logged,4155 fail
logging to 192.168.23.89
logging to 2000::1
Delay-send logging: 2641 message lines logged
logging to 192.168.23.89 by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z Hostname SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z Hostname SYS 6 SHELL_LOGIN [USER@4881
name="" type="" from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z Hostname CAPWAP 4 NO_IP_ADDR - No ip
address for capwap.
<135>1 2013-07-24T12:20:02.80343Z Hostname - 7 - - Please config the IP
address for capwap.
<132>1 2013-07-24T12:20:02.80313Z Hostname CAPWAP 4 NO_IP_ADDR - No ip
address for capwap.
<135>1 2013-07-24T12:19:33.130290Z Hostname - 7 - - Please
config the IP address for capwap.
    
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

**Related Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

**Platform Description** N/A

### 1.43 terminal monitor

Use this command to show logs on the current VTY window. Use the **no** form of this command to restore the default setting.

**terminal monitor**

**terminal no monitor**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Log information is not allowed to be displayed on the VTY window by default.

**Command Mode** Privileged EXEC mode

**Usage Guide** This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.

**Configuration Examples** The following example allows log information to be printed on the current VTY window:

```
Hostname# terminal monitor
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

Command History	Version	Description
	N/A	N/A

# 1 Software Upgrade Commands

## 1.1 show component

Use this command to display all components already installed on current device and their information.


**show component** [ *component\_name* ]

Parameter Description	Parameter	Description
	<i>component_name</i>	Name of the components When this parameter value is N/A, the command is used to display all components already installed on the device and basic information of these components. When this parameter value is not N/A, the command is used to display detailed information of the corresponding component, check whether the component is intact, and check whether this component works properly.

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command includes one with *component\_name* and one without *component\_name*. During upgrade, it requires users to understand all components installed on current device and their version information before components deletion. This needs to use the **show component** command without *component\_name*. The **show component** command with *component\_name* is used to obtain details of the corresponding component. The detailed information enables users to easily realize components' operation and damage. It is significant to insure their troubleshooting, security and reliability.

 Some components in use will change their defaults files. Though this is more possibly normal than malicious, the **show component** command is used only to judge whether component files change in use. It is unable to distinguish natural damage from malicious one. It depends on users to make a further judgment.

**Configuration** The following example displays all components already installed on the information.

**Examples**

```

Hostname# show component
Package :sysmonit
      Version:1.0.1.23cd34aa      Build time: Wed Dec 7 00:58:56 2013
      Size:12877  Install time :Wed Mar 5 14:23:12 2012
    
```

```

Description: this is a system monit package
Required packages: None
-----
Package:bridge
  Version:2.0.1.37cd5cda      Build time: Wed Dec 7 00:54:56 2013
  Size:23245  Install time :Wed  Mar 5 14:30:12 2012
  Description: this is a bridge package
  Required packages: None
-----
    
```

This command is used to obtain all components already installed on the device and their basic information. The information offers a basis for users to decide whether to upgrade or delete components.

Field	Description
Package	Name of the component
Version	Version number of the component
Build time	Compilation time of the component on the server
Size	Content size of the component
Install time	Installation time of the component
Description	Simple functional description of the component
Required packages	Name of required packages

The following example displays the information of specified components already installed.

```

Hostname# show componentbridge
package:bridge
  Version: 2.3.1.1252ea      Build time: Wed Dec 7 00:54:56 2013
  Size:26945  Install time : Wed Mar 19:23:15 2012
  Description:this is a bridge package
  Required packages: None
  Package files:
    /lib64
    /lib64/libbridge.so
    /sbin
    /sbin/bridge

  Package file validate: [OK]
  Required relationship verify: [OK]
    
```

The other information except basic information of components is listed as follows.

Field	Description
-------	-------------

Package file validate	Checks whether the component files are intact. "OK" is displayed when all component files work properly; "ERR" is displayed together with their names when some component files are lost or revised.
Required package	Lists all required packages of the component. "OK" is labeled if required components are already installed; "ERR" is labeled if not together with detailed description about their names and versions.
Package files	Lists all files contained in the package.

**Prompt**

The execution is successful with all components information displayed.

**Messages**

```
Package :sysmonit
  Version:1.0.1.23cd34aa      Build time: Wed Dec 7 00:58:56 2013
  Size:12877  Install time :Wed  Mar 5 14:23:12 2012
  Description: this is a system monit package
  Required packages: None
-----
Package:bridge
  Version:2.0.1.37cd5cda      Build time: Wed Dec 7 00:54:56 2013
  Size:23245  Install time :Wed  Mar 5 14:30:12 2012
  Description: this is a bridge package
  Required packages: None
-----
```

## 1.2 show patch

Use this command to display information about the installed hot patch.

**show patch** [ *patch\_name* ]

**Parameter Description**

Parameter	Description
<i>patch_name</i>	Indicates the patch name. When this parameter is not specified, the command is used to display all installed patches and basic information about each patch on the device. When this parameter is specified, the command is used to display detailed information about the corresponding patch and content of the patch, and to check whether the content of the component is complete.

**Command Mode**

Privileged EXEC mode



**Default Level** 2

**Usage Guide** This command can be used to display installed patches and patch information.

**Configuration** 1 . The following example displays installed patches on a fixed device.

**Examples**

```

Hostname# show patch
Patch package SP2 installed in the system, version:pa
  Order      : 2
  -----
  Patch      : patch_utils
  Status     : installed
  Version    : 1.0.0.70a1a80
  Size       : 239273
  Build time : Thu May 9 06:13:33 2019
  Install time: Fri May 10 11:21:31 2019
  Description : utils patch
    
```

Use this command to obtain basic information about all installed patches.

Field	Description
order	Patch installation serial number
Package	Patch name
status	Patch status
Version	Version number of the component
Build time	Compilation time of the component on the server
Size	Content size of the component
Install time	Installation time of the component
Description	Brief description of the patch function

The other information except basic information of components is listed as follows.

Field	Description
Package file validate	Checks integrity of files contained in the package. If all files are normal, the result is displayed as OK; if some files are lost or modified, the result is displayed as ERR and the file that is lost or modified is listed.
Package files	Lists all files contained in the package.

**Prompt** 执行后显示设备存在的补丁信息。 Information about patches on the device is displayed.

**Messages**

```

Patch package patch_install installed in the system, version:pal
Package : patch_bridge
Status : running
Version: pal      Build time: Mon May 13 09:03:07 2013
  Size: 277      Install time: Tue May 21 03:07:17 2013
  Description: a patch for bridge
  Required packages: None
    
```

### 1.3 show upgrade file

Use this command to display the information of the installation package files in the device file system.


**show upgrade file** *url*

Parameter Description	Parameter	Description
	<i>url</i>	The local <i>url</i> path indicates where an installation package file is stored.

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to preview main messages of an installation package after it is downloaded into local file system.

 This command is not applied to a chassis package.

**Configuration** The following example displays the information of an installation package file.

**Examples**

```

Hostname# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name      : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target    : eg1000m
Size              : 26945
Build time        : Wed Dec 7 00:54:56 2013
Install date      : (not installed)
Description       : this is a bridge package
Package files :
    Package files:
        /lib64
        /lib64/libbridge.so
        /sbin
        /sbin/bridge
    
```

This command is used to obtain the information in the package.

Field	Description
Name	Name of the package
Version	Version of the package
Package type	Type of the package
Support target	Supported product description
Size	Content size of the package

Build time	Compilation time of the package
Install date	Installation time of the package
Description	Description of the package
Package files	All contents in the package

**Prompt** The package information is displayed after running.

**Messages**

```
Name      : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target    : eg1000m
Size              : 26945
Build time       : Wed Dec 7 00:54:56 2013
Install date     : (not installed)
Description      : this is a bridge package
Package files :
    Package files:
        /lib64
        /lib64/libbridge.so
        /sbin
        /sbin/bridge
```

## 1.4 upgrade download tftp

Use this command to download, install and upgrade installation packages from the tftp server.

**upgrade download tftp:/path [ force ]**

**Parameter Description**

Parameter	Description
<i>path</i>	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
<b>force</b>	Enforces upgrade.

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is applicable to installation packages of all subsystem components and feature components. This command is used to perform automatic installation, copy and upgrade of files.

**Configuration** The following example upgrades the main package.

**Examples**

```
Hostname# upgrade download
tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Upgrade processing is 10%
Upgrade processing is 60%
Upgrade processing is 90%
Upgrade info [OK]
    Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
    Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
Upgrade processing is 100%
Reload to take effect!

```

**Verification** Run the **show version detail** command to check whether the upgrade of a subsystem component is successful.

Run the **show component** command to check whether the upgrade of a feature component is successful.

**Prompt** The prompt message of successful running is displayed.

**Messages** Upgrade info [OK];

The installation package is invalid or damaged and needs to be regained for upgrade command.

Invalid package file

The installation package is not available on the device and needs to be regained for upgrade command.

Device don't support

There is no need to upgrade the device.

The version in device is newer or the same

When there is insufficient space for upgrade, check USB flash disk attached on the device.

No enough space for decompress

Contact the service center to solve the system problem.

No enough space,rootfs been destroyed. Please upgrade in uboot

The existing patch package needs to be deleted.

Already exist patch, please uninstall before upgrade

The patch package is not compatible on this device. Replace the package.

Patch compatibility err

The upgrade of the patch package is not applied to the device. Regain the package.

```
Some origin component has change
```

## 1.5 upgrade rollback

Use this command to roll a subsystem back to the version before the upgrade.


### upgrade rollback

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used when the device cannot work properly after subsystem upgrade. It takes effect only when the last upgrade of subsystem components is successful.

 The command is valid after device restart. The recursive rollback cannot be executed through this command in succession.

**Configuration Examples** The following example rolls a subsystem back to the version before the upgrade on the box device.

```
Hostname#upgrade rollback
kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21] [OK]
rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537] [OK]
Rollback success!
Reload system to take effect!
```

**Verification** Run the **show version detail** command to check the result of rolling back subsystem components after device restart.

**Prompt Messages** The prompt message of successful running is displayed.

```
Rollback success!
Restart to take effect !
```

The rollback operation cannot be performed when subsystem components have not been upgraded last time.

```
Not subsys package last upgrade
```

The rollback operation cannot be performed for the last upgrade is not successful.

```
Last upgrade err or skip
```

The upgrade command has not been run or the rollback operation has been performed.

```
Monitor file lost
```

**Common Errors** The last upgrade is not for subsystem components, but for feature packages, hot patch packages and so on.  
Run the rollback command for subsystem once.

## 1.6 clear storage

Use this command to remove an installation package on the local device.

**clear storage** [ *url* ]

Parameter Description	Parameter	Description
	<i>url</i>	A local <i>url</i> directory or full path name indicates where the installation package is stored

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to remove an installation package or all packages in a directory and all installation packages on the local device.

**Configuration** Hostname#clear storage

**Examples**  
 Remove the whole storage directory?[y/n]y  
 Hostname#clear storage usb0  
 Remove the file or directory usb0 from the storage?[y/n]y  
 Hostname#

**Verification** Check specified *url*

**Platforms** N/A

# 1 Time Range Commands

## 1.1 absolute

Use this command to configure an absolute time range.

**absolute** { [ *start time date* ] [ *end time date* ] }

Use the **no** form of this command to remove the absolute time range.

**no absolute**

Parameter Description	Parameter	Description
	<b>start</b> <i>time date</i>	Indicates the start time of the range.
	<b>end</b> <i>time date</i>	Indicates the end time of the range.

**Defaults** No absolute time range is configured by default. In this case, the maximum time range is used.

**Command Mode** Time range configuration mode

**Default Level** 14

**Usage Guide** Use the **absolute** command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range.  
The maximum time range is from 0000-01-01 00:00 to 9999-12-31 23:59.

**Configuration Examples** The following example creates a time range and enters time range configuration mode.

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

The following example configures an absolute time range.

```
Hostname(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

**Check Method** Use the **show time-range** [ *time-range-name* ] command to display the time range configuration.

**Prompt Message** -

**Platform Description** -

## 1.2 periodic

Use this command to configure the periodic time.

**periodic** *day-of-the-week time to [ day-of-the-week ] time*

Use the **no** form of this command to remove the configured periodic time.

**no periodic** *day-of-the-week time to [ day-of-the-week ] time*

Parameter Description	Parameter	Description
	<i>day-of-the-week</i>	Indicates the week day when the periodic time starts or ends.
	<i>time</i>	Indicates the exact time when the periodic time starts or ends.

**Defaults** No periodic time is configured by default.

**Command Mode** Time range configuration mode

**Default Level** 14

**Usage Guide** Use the **periodic** command to configure a periodic time interval to allow a certain function to take effect within the periodic time.  
 Before modifying a period for a service, you are advised to disassociate the time range. After the period is modified, associate the time range again.

**Configuration Examples** The following example creates a time range and enters time range configuration mode.

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

The following example configures a periodic time interval.

```
Hostname(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

**Check Method** Use the **show time-range [ time-range-name ]** command to display the time range configuration.

**Prompt Message** -

**Platform Description** -



### 1.3 show time-range

Use this command to display the time range configuration.

**show time-range** [ *time-range-name* ]

Parameter Description	Parameter	Description
	<i>time-range-name</i>	Displays a specified time range.

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** Use this command to check the time range configuration.

**Configuration** The following example displays the time range configuration.

**Examples**

```

Hostname# show time-range
time-range entry: test (inactive)
  absolute end 01:02 02 February 2012
    
```

**Prompt Message** -

**Platform Description** -

### 1.4 time-range

Use this command to create a time range and enter time range configuration mode.

**time-range** *time-range-name*

Use the **no** form of this command to remove the configured time range.

**no time-range** *time-range-name*

Parameter Description	Parameter	Description
	<i>time-range-name</i>	Time range name

**Defaults** No time range is configured by default.

**Command Mode** Global configuration mode

**Default Level** 2

**Usage Guide** Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range. After the time range is created, you can configure relevant time control in time range mode.

**Configuration** The following example creates a time range.

**Examples**

```
Hostname(config)# time-range no-http
Hostname(config-time-range)#
```

**Check Method** Use the **show time-range** [ *time-range-name* ] command to display the time range configuration.

**Prompt Message** -

**Platform Description** -



# Interface Commands

---

1. Ethernet Interface Commands

# 1 Ethernet Interface Commands

## 1.1 bandwidth

Use this command to set the bandwidth on the interface. Use the **no** form of this command to restore the default setting.

**bandwidth** *kilobits*

**no bandwidth**

### Parameter Description

Parameter	Description
<i>kilobits</i>	Bandwidth per second, in the range from 1 to 2147483647 in the unit of Kbps.

### Defaults

If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.

### Command Mode

Interface configuration mode

### Usage Guide

This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.

### Configuration Examples

The following example sets the bandwidth on the interface to 64 Kbps.

### Examples

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# bandwidth 64

```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.2 carrier-delay

Use this command to set the carrier delay on the interface. Use the **no** form of this command to restore the default value.

**carrier-delay** { *num* }

**no carrier-delay**

Parameter Description	Parameter	Description
	<i>num</i>	Second-level carrier delay of the interface, in seconds. The value range is from 0 to 60.

**Defaults** The default is 2 seconds.

**Command Mode** Interface configuration mode

**Usage Guide** The carrier delay refers to the delay after which the DCD signal changes from **Down** to **Up** or from **Up** to **Down**. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation.

If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.

**Configuration Examples** The following example sets the carrier delay of serial interface to 5 seconds.

**Examples**

```

Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# carrier-delay 5

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.3 clear counters

Use this command to clear the counters on the specified interface.

**clear counters** [ *interface-type interface-number* ]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Type and number of the interface.

**Defaults** N/A

**Command** Privileged EXEC mode.  
**Mode**

**Usage Guide** In the privileged EXEC mode, use the **show interfaces** command to display the counters or the **clear counters** command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.

**Configuration** The following example clears the counters on GigabitEthernet 0/1.

**Examples**

```
Hostname# clear counters GigabitEthernet 0/1
```

**Related Commands**

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A  
**Description**

## 1.4 clear interface

Use this command to reset the interface hardware.

**clear interface** *interface-type interface-number*

**Parameter Description**

Parameter	Description
<i>interface-type</i>	Interface type.
<i>interface-number</i>	Interface ID.

**Defaults** N/A

**Command** Privileged EXEC mode.  
**Mode**

**Usage Guide** This command is only used on the switch port, member port of the L2 aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the **shutdown** and **no shutdown** commands.

**Configuration** The following example resets GigabitEthernet 0/1.

**Examples**

```
Hostname# clear interface GigabitEthernet 0/1
```

**Related Commands**

Command	Description
<b>shutdown</b>	Disables the interface.

**Platform** N/A  
**Description**

## 1.5 description

Use this command to configure the alias of interface. Use the **no** form of this command to restore the default setting.

**description** *string*  
**no description**

Parameter Description	Parameter	Description
	<i>string</i>	Interface alias, which has up to 80 characters.

**Defaults** No alias is configured by default.

**Command Mode** Interface configuration mode.

**Usage Guide** Use **show interfaces** to display the interface information, including the alias.

**Configuration Examples** The following example configures the description of GigabitEthernet 0/1 as **GBIC-1**.

### Examples

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# description GBIC-1

```

Related Commands	Command	Description
	<b>show interfaces</b>	Displays the interface information.

**Platform** N/A  
**Description**

## 1.6 duplex

Use this command to specify the duplex mode for the interface. Use the **no** form of this command to restore the default setting.

**duplex** { **auto** | **full** | **half** }  
**no duplex**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<b>auto</b>	Self-adaptive full duplex and half duplex.
<b>full</b>	Full duplex.
<b>half</b>	Half duplex.

**Defaults** The interface is in auto-negotiation mode.

**Command** Interface configuration mode

**Mode**

**Usage Guide** The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

**Configuration** The following example configures the full duplex mode for GigabitEthernet 0/1.

**Examples**

```

Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# duplex full

```

**Related  
Commands**

Command	Description
<b>show interfaces</b>	Displays the interface information.

**Platform** N/A

**Description**

## 1.7 encapsulation dot1q

Use this command to encapsulate IEEE 802.1Q in interface mode. Use the **no** form of this command to restore the default setting.

**encapsulation dot1Q** *VLAN-ID*

**no encapsulation**

**Parameter  
Description**

Parameter	Description
<i>VLAN-ID</i>	Indicates the VLAN ID. The value is an integer that ranges from 1 to 4094.

**Defaults** The encapsulation protocol is IEEE802.1Q by default, and no VLAN is encapsulated.

**Command** Sub-interface configuration mode

**Mode**

**Usage Guide** 802.1Q is an IEEE standard protocol used to communicate between Layer 2 and Layer 3 devices that have been assigned to VLANs.



802.1Q encapsulation can be only configured on Ethernet sub-interfaces. Wired main interfaces of the AP support this function.

**Configuration** The following example configures 802.1Q on GigabitEthernet 0/1.20 and set the VLAN ID to 20.

**Examples** `Hostname(config)# interface GigabitEthernet 0/1.20`

```
Hostname(config-subif)# encapsulation dot1q 20
```

**Related  
Commands**

Command	Description
N/A	N/A.

**Platform** N/A.

**Description**

## 1.8 interface

Run this command to enter the interface configuration mode.

**interface** *interface-type interface-number*

**Parameter  
Description**

Parameter	Description
<i>interface-type</i>	The interface type.
<i>interface-number</i>	Interface ID.

**Defaults** N/A

**Command  
Mode** Global configuration mode

**Usage Guide** You can run this command to enter the interface configuration mode. Then you can modify the interface configuration.

**Configuration** The following example enters the configuration mode of GigabitEthernet 0/1.

**Examples** `Hostname(config)# interface GigabitEthernet 0/1`

```
Hostname(config-if-GigabitEthernet 0/1)#
```

The following example enters the configuration mode of the logical interface VLAN 1.

```
Hostname(config)# interface vlan 1
```

```
Hostname(config-if-VLAN 1)#
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.9 interface range

Run this command to batch configure interfaces.

```
interface range { port-range | macro macro_name }
```

Use this command to define the macro name of the **interface range** command.

```
define interface-range macro_name
```

**Parameter Description**

Parameter	Description
<i>port-range</i>	The interface type and ID range, entered in the form of <i>interface-type slot-number/interface-number</i> . The interface can be either an Ethernet physical interface or a loopback interface.
<b>macro</b> <i>macro_name</i>	The macro name which represents the interface range.

**Defaults** The **interface range** command is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use the **define interface-range** command to define a range of interfaces as the macro name and then use the **interface range macro** *macro\_name* command to enter interface configuration mode on multiple interfaces.

**Configuration Examples** The following example batch sets the bandwidth parameter of GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/4 to 100 kbps.

```
Hostname(config)# interface range gigabitEthernet 0/0, 0/2
Hostname(config-if-range)# bandwidth 100
```

The following example defines the interface macro name of GigabitEthernet 0/1 and GigabitEthernet 0/2 as **route1**, and batch sets the bandwidth parameter to 100 Kbps.

```
Hostname(config)# define interface-range route1 gigabitEthernet 0/0-2
Hostname(config)# interface range macro route1
Hostname(config-if-range)# bandwidth 100
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.10 load-interval

Use this command to set the interval for calculating load on the interface. Use the **no** form of this command to restore the default setting.

**load-interval** *seconds*

**no load-interval**

Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 5 to 600 in the unit of seconds.

**Defaults** The default is 10.

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to set the interval for calculating load on the interface. In general, the numbers of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the **show interface gigabitethernet 0/1** command is run.

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

**Configuration Examples** The following example sets the interval for calculating load on GigabitEthernet 0/1 to 180 seconds.

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# load-interval 180
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.11 logging

Use this command to print information on the interface. Use the **no** form of this command to disable this function.

**logging** [ **link-updown** | **error-frame** | **link-dither** ]

**no logging** [ **link-updown** | **error-frame** | **link-dither** ]

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<b>link-updown</b>	Prints the status change information.
<b>error-frame</b>	Prints the error frame information.
<b>link-dither</b>	Prints the port flapping information.

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** You can decide whether to enable interface information printing. The function is enabled by default. Notifications displayed when the interface state changes, the interface receives an error frame or flaps, the interface drops the received frame due to insufficient resources, and the interface receives a CRC error packet will be printed. The notifications will not be printed after you run the **no logging** [ **link-updown** | **error-frame** | **link-dither** | **res-lack-frame** | **crc-frame** ] command.

**Configuration Examples** The following example prints information on the interface.

```

Hostname(config)# logging link-updown
Hostname(config)# logging error-frame
Hostname(config)# logging link-dither
Hostname(config)# logging res-lack-frame
Hostname(config)# logging crc-frame
Hostname(config)# logging insert-remove
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.12 mtu

Use this command to set the MTU supported on the interface.

**mtu** *num*

Parameter Description	Parameter	Description
	<i>num</i>	64 to 1500

**Defaults** The default is 1500.

**Command** Interface configuration mode.  
**Mode**

**Usage Guide** This command is used to configure the MTU of an interface, that is, the maximum length of a data frame at the link layer. The MTU can be configured on a physical interface only.

**Configuration** The following example sets the MTU of GigabitEthernet 0/1 to 9000.

**Examples**

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet)# mtu 9000
```

**Related Commands**

Command	Description
show interfaces	Displays interface information.

**Platform** N/A  
**Description**

## 1.13 physical-port dither protect

Use this command to enable swapping protection on the port. Use the **no** form of this command to disable this function.

**physical-port dither protect**  
**no physical-port dither protect**


**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After you configure the **physical-port dither protect** command, the port will be shut down when the swapping occurs for certain times. If you run the **no physical-port dither protect** command, prompts are printed and the port is not shut down.

 If swapping occurs on the port for 6 times within 2 seconds, a syslog will be printed. If syslog is printed for 10 consecutive times, the port will be shut down. If swapping occurs on the port for over 10 times within 10 seconds, a syslog will be printed but the port will not be shut down.

**Configuration** The following example enables swapping protection on the port.

**Examples**

```
Hostname(config)# physical-port dither protect
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.14 show interfaces

Use this command to display the interface information and optical module information.

**show interfaces** [ *interface-type interface-number* ] [ **description** [ **up** | **down** ] ]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Type and number of the interface.
	<b>description</b>	Description of the interface, including the link status. up: displays the statistics of the interface in <b>Up</b> state. down: displays the statistics of the interface in <b>Down</b> state.

### Defaults

**Command** All modes except the user EXEC mode  
**Mode**

**Usage Guide** This command is used to show basic information if no parameter is specified.

**Configuration** The following example displays information about GigabitEthernet 0/1 used as the trunk interface.

### Examples

```

Hostname# show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
Interface address is: no ip address
Interface IPv6 address is:
No IPv6 address
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec

```

## Ethernet attributes:

```
Last link state change time: 2012-12-22 14:00:48
Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
Priority is 0
Medium-type is Copper
Admin duplex mode is AUTO, oper duplex is Unknown
Admin speed is AUTO, oper speed is Unknown
Flow receive control admin status is OFF, flow send control admin status is OFF
Flow receive control oper status is Unknown, flow send control oper status is Unknown
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
```

## Bridge attributes:

```
Port-type: trunk
Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
```

```
Queueing strategy: FIFO
```

```
Output queue 0/0, 0 drops;
```

```
Input queue 0/75, 0 drops
```

```
Rxload is 1/255 ,Txload is 1/255
```

```
5 minutes input rate 0 bits/sec, 0 packets/sec
```

```
5 minutes output rate 0 bits/sec, 0 packets/sec
```

```
0 packets input, 0 bytes, 0 no buffer, 0 dropped
```

```
Received 0 broadcasts, 0 runts, 0 giants
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
0 packets output, 0 bytes, 0 underruns , 0 dropped
```

```
0 output errors, 0 collisions, 0 interface resets
```

The following example displays information about GigabitEthernet 0/1 used as the access interface.

```
Hostname#show interfaces GigabitEthernet 0/1
```

```
Index(dec):1 (hex):1
```

```
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
```

```
Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
```

```
Interface address is: no ip address
```

```
Interface IPv6 address is:
```

```
No IPv6 address
```

```
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Ethernet attributes:
  Last link state change time: 2012-12-22 14:00:48
  Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
  Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
  Priority is 0
  Medium-type is Copper
  Admin duplex mode is AUTO, oper duplex is Unknown
  Admin speed is AUTO, oper speed is Unknown
  Flow receive control admin status is OFF,flow send control admin status is OFF
  Flow receive control oper status is Unknown,flow send control oper status is Unknown
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
  Port-type: access
  Vlan id : 2
Queueing strategy: FIFO
  Output queue 0/0, 0 drops;
  Input queue 0/75, 0 drops
Rxload is 1/255, Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

The following example displays information about GigabitEthernet 0/1 used as the hybrid interface.

```
Hostname#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet
```



```
Interface address is: no ip address
Interface IPv6 address is:
  No IPv6 address
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Ethernet-II, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Ethernet attributes:
  Last link state change time: 2012-12-22 14:00:48
  Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
  Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
  Priority is 0
  Medium-type is Copper
  Admin duplex mode is AUTO, oper duplex is Unknown
  Admin speed is AUTO, oper speed is Unknown
  Flow receive control admin status is OFF,flow send control admin status is OFF
  Flow receive control oper status is Unknown,flow send control oper status is Unknown
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Bridge attributes:
  Port-type: hybrid
  Tagged vlan id:2
  Untagged vlan id:none
Queueing strategy: FIFO
  Output queue 0/0, 0 drops;
  Input queue 0/75, 0 drops
Rxload is 1/255 ,Txload is 1/255
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  0 packets output, 0 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

The following example displays information about GigabitEthernet 0/1.

```

Hostname# show interfaces GigabitEthernet 0/1 switchport
Interface                Switchport Mode      Access Native Protected VLAN lists
-----
GigabitEthernet 0/1     enabled    ACCESS    2      1      Disabled ALL
    
```

**Related Commands**

Command	Description
<b>duplex</b>	Duplex
<b>flowcontrol</b>	Flow control status.
<b>interface gigabitethernet</b>	Selects the interface and enter the interface configuration mode.
<b>interface aggregateport</b>	Creates or accesses the aggregate port, and enters the interface configuration mode.
<b>interface vlan</b>	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
<b>shutdown</b>	Disables the interface.
<b>speed</b>	Configures the speed on the port.
<b>switchport priority</b>	Configures the default 802.1q interface priority.
<b>switchport protected</b>	Configures the interface as a protected port.

**Platform** N/A  
**Description**

### 1.15 show interfaces counters

Use this command to display the received and transmitted packet statistics.

```

show interfaces [ interface-type interface-number ] counters [ increment | error | rate | summary ]
[ up | down ]
    
```

**Parameter Description**

Parameter	Description
<i>interface-type interface-number</i>	(Optional) The interface type and ID. If the interface type and number are not specified, the statistics of all interfaces are displayed.
<b>increment</b>	Displays the packet statistics increased during the last sample interval.
<b>errors</b>	Displays error packet statistics.
<b>drops</b>	Displays the statistics of dropped packets.
<b>rate</b>	Displays packet receiving and transmitting rate.
<b>summary</b>	Displays packet statistics summary.
<b>up</b>	(Optional) Displays the statistics of the interface in <b>Up</b> state.
<b>down</b>	(Optional) Displays the statistics of the interface in <b>Down</b> state.

<b>nozero</b>	Displays the statistics of the interface with some statistical values of interface packet quantity not equal to 0.
---------------	--

**Defaults** N/A

**Command** All modes except the user EXEC mode

**Mode**

**Usage Guide** If you do not specify an interface, the packet statistics on all interfaces are displayed.

**Configuration** The following example displays packet statistics on interface GigabitEthernet 0/1.

**Examples**

```

Hostname# show interfaces gigabitethernet 0/1 counters
Interface : GigabitEthernet 0/1
5 minute input rate : 9144 bits/sec, 9 packets/sec
5 minute output rate : 1280 bits/sec, 1 packets/sec
Rxload          : 1%
InOctets        : 17310045
InPkts          : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts    : 100
InMulticastPkts : 100
InBroadcastPkts : 800
Txload          : 1%
OutOctets       : 1282535
OutPkts         : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts   : 100
OutMulticastPkts : 100
OutBroadcastPkts : 800
Undersize packets : 0
Oversize packets : 0
collisions      : 0
Fragments       : 0
Jabbers         : 0
CRC alignment errors : 0
AlignmentErrors : 0
FCSErrors       : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
 64:46264
 65-127: 47427
128-255: 3478
256-511: 658
512-1023: 18016
1024-1518: 125
Packet increment in last sampling interval(5 seconds):

```

```

InOctets      : 10000
InPkts       : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts  : 100
InMulticastPkts : 100
InBroadcastPkts : 800
OutOctets     : 10000
OutPkts      : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts : 100
OutMulticastPkts : 100
    
```

- i** Rxload refers to the receive bandwidth usage and Txload refers to the Tx bandwidth usage. InPkts is the total number of receive unicast, multicast and broadcast packets. OutPkts is the total number of transmit unicast, multicast and broadcast packets. Packet increment in last sampling interval (5 seconds) represents the packet statistics increased during the last sample interval (5 seconds).

The following example displays the packet statistics on interface GigabitEthernet 0/1 increased during the last sample interval.

```

Hostname# show interfaces gigabitethernet 0/1 counters increment
Interface : GigabitEthernet 0/1
Packet increment in last sampling interval(5 seconds):
  InOctets      : 10000
  InPkts       : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts  : 100
  InMulticastPkts : 100
  InBroadcastPkts : 800
  OutOctets     : 10000
  OutPkts      : 1000 (Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts : 100
  OutMulticastPkts : 100
    
```

The following example displays error packet statistics on interface GigabitEthernet 0/1.

```

Hostname# show interfaces gigabitethernet 0/1 counters increment
Interface  UnderSize      OverSize      Collisions
Fragments
-----
-
Gi0/1      0                0                0                0
Interface  Jabbers      CRC-Align-Err  Align-Err      FCS-
Err
-----
-
Gi0/1      0                0                0                0
    
```

- i** UnderSize: indicates the number of valid packets smaller than 64 bytes.
- OverSize: indicates the number of valid packets smaller than 1518 bytes.
- Collisions: indicates the number of colliding transmit packets. Fragments: indicates the number

of packets with CRC error or frame alignment error which are smaller than 64 bytes.

Jabbers: indicates the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.

CRC-Align-Err: indicates the number of receive packets with CRC error.

Align\_Err: indicates the number of receive packets with frame alignment error.

FCS-Err: indicates the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on GigabitEthernet 0/1.

```

Hostname# show interface gigabitethernet 0/1 counters rate
Interface      Sampling Time      Input Rate          Input Rate
Output Rate    Output Rate
                (bits/sec)         (packets/sec)
(bits/sec)     (packets/sec)
-----
Gi0/1          5 seconds          23391              23
124            0
  
```

- Sampling Time is the time when packets are sampled. Input rate is packet receiving rate and Output rate is packet transmitting rate.

The following example displays packet statistics summary on GigabitEthernet 0/1.

```

Hostname# show interface gigabitethernet 0/1 counters summary
Interface      InOctets           InUcastPkts        InMulticastPkts
InBroadcastPkts
-----
Gi0/1          1475788005         1389               45880503
11886621
Interface      OutOctets           OutUcastPkts        OutMulticastPkts
OutBroadcastPkts
-----
Gi0/1          6667915            6382               31629
13410
  
```

- InOctets is the total number of packets received on the interface. InUcastPkts is the number of unicast packets received on the interface. InMulticastPkts is the number of multicast packets received on the interface. InBroadcastPkts is the number of broadcast packets received on the interface.

OutOctets is the total number of packets transmitted on the interface. OutUcastPkts is the number of unicast packets transmitted on the interface. OutMulticastPkts is the number of multicast packets transmitted on the interface. OutBroadcastPkts is the number of broadcast packets transmitted on the interface.

The following example displays the statistics of the dropped packets on GigabitEthernet 0/1.

```

Hostname # #show interface gigabitEthernet 1/0/6 counters drops
  
```

```

Interface : GigabitEthernet 1/0/6

Input dropped packets          : 2453
Input no buffer packets       : 0
Input qos dropped packets     : 0
Output dropped packets       : 0
Output no buffer packets     : 0
Forwarding entry dropped packets : 2453
    
```

Field	Description
Input dropped	Indicates the number of received packets that are dropped, excluding the packets dropped due to QoS restrictions or insufficient resources.
Input no buffer	Indicates the number of received packets that are dropped due to insufficient resources.
Input qos dropped	Indicates the number of received packets that are dropped due to QoS receiving restrictions.
Output dropped packets	Indicates the number of packets dropped during transmission.
Output no buffer	Indicates the number of packets that cannot be sent successfully due to lack of resources.
Forwarding entry dropped	Indicates the total number of packets dropped during forwarding, including packets dropped at the ingress and egress. The calculation formula is:  Number of packets dropped at the ingress + Number of packets dropped at the egress - Number of no buffer packets at the ingress - Number of no buffer packets at the egress - Number of CRC error packets.

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

## 1.16 show interfaces ethernet brief

Use this command to display brief information of interfaces, including interface status, output and input bandwidth usage, and the numbers of output and input packet errors.

**show interfaces** { *interface-type interface-number* **ethernet brief** | **ethernet brief** [ **up** | **down** ] }

**Parameter Description**

Parameter	Description
<i>interface-type interface-number</i>	Specifies interface type and interface number. Information of all interfaces are displayed if this field is not specified.
<b>up</b>	(Optional) Displays the brief information when the port is up.
<b>down</b>	(Optional) Displays the brief information when the port is down.

**Command Mode** All modes except the user EXEC mode

**Default Level** 14

**Usage Guide** If no interface name is specified, Ethernet information about all interfaces is displayed, including the link status, VLAN to which the interface belongs, auto-negotiation mode, duplex mode, interface speed, bandwidth usage, and description (alias).  
The interface type can be the physical interface, aggregate interface, or management interface.

**Configuration Examples** The following example displays brief information about GigabitEthernet 0/1.

```

Hostname#show interfaces GigabitEthernet 0/1 ethernet brief
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex  Speed  Input Usage  Output Usage
Description
-----
-----
Gi0/1      down      1     OFF       Unknown Unknown  0.00%      0.00%
10G port  0.01%
```

Link Stat: indicates the link status of the interface. If the value is disabled, you can run the **show interface status err-disabled** command to check the cause of the errdisable state. If the value is \*down, the **shutdown** command is configured on the interface.

Vlan: indicates the VLAN to which the interface belongs.





Gi0/3	down	1	OFF	Unknown	Unknown	0.00%	0.00%
Ag1	up	1	OFF	Full	1000M	46.78%	46.77%
Mg0	up	routed	--	Full	1000M	--	--
IP management Console							

### 1.17 show interfaces link-state-change statistics

Run this command to view the change time and count of the interface link state.

**show interfaces** [ *interface-type interface-number* ] **link-state-change statistics**

**Parameter Description**

Parameter	Description
<i>interface-type interface-number</i>	Type and number of the interface. If the interface type and number are not specified, the details of all interfaces are displayed.

**Command Mode** All modes except the user EXEC mode

**Default Level** 14

**Usage Guide** If no interface name is specified, the link state change information of all the interfaces are displayed.

**Configuration Examples** The following example displays the link state change information of an interface.

```

Hostname# show int link-state-change statistics
Interface   Link state Link state change times   Last change time   Link-dither begin
Link-dither end
-----
-----
Te0/1       down       0                           2018-05-05 11:07:45  none
none
    
```

Field	Description
Link state change times	Indicates the link state change times of the interface. You can run the <b>clear link-state-change statistics</b> <i>interface-type interface-number</i> command to clear it.

<i>interface-number</i>	Indicates the last link state change time of the interface.
Link-dither begin	Indicates the start time of the last detected frequent link flapping. The value <b>none</b> indicates that no frequent link flapping occurs.
Link-dither end	Indicates the end time of the last detected frequent link flapping. The value <b>none</b> indicates that no frequent link flapping occurs. Condition of frequent link flapping: the link of the port flaps six times in 2s (the same as the condition of port flapping protection).  After frequent port flapping (six times in 2s) is detected, the detection time is recorded as the start time of frequent flapping ( <b>Link-dither begin</b> ), and the detection continues in 2s. If no frequent port flapping is detected in 2s, or after the port is shut down by flapping protection, the detection time is recorded as the end time of frequent flapping ( <b>Link-dither end</b> ).

**Notifications** N/A

**Platform** N/A

**Description**

## 1.18 show interfaces status

Run this command to view the status information of an interface.

**show interfaces** [ *interface-type interface-number* ] **status**

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Type and number of the interface.
	<b>status</b>	Displays status information of the interface, including the rate and duplex mode.

**Command Mode** All modes except the user EXEC mode

**Default Level** 14

**Usage Guide** If no interface name is specified, the state information of all the interfaces is displayed.

**Configuration Examples** The following example displays the status information of the interface GigabitEthernet 0/1.

```

Hostname#show interfaces GigabitEthernet 0/1 status
Interface          Status      Vlan      Duplex  Speed  Type
-----
GigabitEthernet 0/1  up         1         Full    1000M  copper
    
```

**Notifications** N/A

**Platform Description** N/A

### 1.19 show interfaces usage

Run this command to view the bandwidth usage of an interface.

**show interfaces** [ *interface-type interface-number* ] **usage** [ **up** | **down** ]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Type and number of the interface. If the interface type and number are not specified, the statistics of all interfaces are displayed.
	<b>up</b>	(Optional) Displays the bandwidth usage of the interface in <b>Up</b> state.
	<b>down</b>	(Optional) Displays the bandwidth usage of the interface in <b>Down</b> state.

**Command Mode** All modes except the user EXEC mode

**Default Level** 14

**Usage Guide** If no interface name is specified, the bandwidth usage information of all the interfaces is displayed. The bandwidth here refers to the actual link bandwidth rather than the configured bandwidth value on the interface. The support to parameters varies for the L2 and L3 interfaces. The actual support conditions of specific interfaces prevail.

**Configuration Examples** The following example displays the bandwidth usage information of the interface GigabitEthernet 0/1.

```

Interface          Bandwidth  Average Usage  Input Usage  Output
Usage
    
```

-----				
-----				
GigabitEthernet 0/0	1000 Mbit	55.25%	50.00%	60.50%

Field	Description
Interface	Indicates the interface name.
Bandwidth	Indicates the bandwidth of the interface link, that is, the maximum rate of the link.
Average Usage	Indicates the current bandwidth usage.
Input Usage	Indicates the receiving bandwidth usage.
Output Usage	Indicates the transmission bandwidth usage.

**Notifications** N/A

**Platform** N/A

**Description**

## 1.20 show vlans

Run this command in privileged EXEC mode to view information about VLAN sub-interfaces.

**show vlans** [ *VLANID* ]

Parameter Description	Parameter	Description
	<i>VLANID</i>	Indicates the VLAN ID. If this parameter is not specified, information about sub-interfaces of all VLANs is displayed.

**Command Mode** All modes except the user EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example displays information about VLAN sub-interfaces.

```

Hostname# show vlans
Virtual LAN ID: 3 (IEEE 802.1Q Encapsulation)
VLAN Interface GigabitEthernet 0/1.1
    
```

```

IP address: 1.1.1.1
Received:30 packets,
Transmitted: 30 packets
Virtual LAN ID: 4 (IEEE 802.1Q Encapsulation)
VLAN Interface GigabitEthernet 0/1.2
IP address: 1.1.2.1
Received:0 packets,
Transmitted: 0 packets
    
```

Virtual LAN ID: indicates the VLAN ID.  
 VLAN Interface: indicates the sub-interface in the VLAN.  
 Address: indicates the IP address of the sub-interface.  
 Received: indicates the number of received packets.  
 Transmitted: indicates the number of sent packets.

**Notifications** N/A

**Platform Description** N/A

## 1.21 shutdown

Run this command to shut down a specific interface  
**shutdown**

Run this command to enable the interface.  
**no shutdown**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, the administrative status of an interface is Up.

**Command Mode** Interface configuration mode

**Usage Guide** You can run the command to shut down interfaces (including Ethernet ports, APs, and SVIs). Other configurations of the interfaces still exists, but does not work. You can run the **show interfaces** command to view the interface status.

To prevent unwanted link flapping caused by frequent operation of the shutdown/no shutdown command, there should be a certain time interval (which must be greater than the carrier delay of the interface) before/after configuring the shutdown/no shutdown command twice on an interface.

**Configuration** The following example shuts down Aggregateport 1.

**Examples**

```
Hostname(config)# interface Aggregateport 1
Hostname(config-if-Aggregateport 1)# shutdown
```

The following example enables Aggregateport 1.

```
Hostname(config)# interface Aggregateport 1
Hostname(config-if-Aggregateport 1)# no shutdown
```

**Related  
Commands**

Command	Description
<b>clear interface</b>	Resets the hardware.
<b>show interfaces</b>	Displays interface information.

**Platform** N/A

**Description**

## 1.22 snmp-server if-index persist

Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.

**snmp-server if-index persist**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command  
Mode** Global configuration mode

**Usage Guide** After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.

**Configuration** The following example enables the interface index persistence.

**Examples**

```
Hostname(config)# snmp-server if-index persist
```

**Related  
Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

**Platform** N/A  
**Description**

## 1.23 snmp trap link-status

Run this command to configure the link trap sending function for an interface. When the function is enabled, the SNMP module sends link traps if the link status changes on the interface.

**snmp trap link-status**

If this function is disabled, the SNMP module does not send link traps.

**no snmp trap link-status**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** This command is used to configure the link trap sending function for an interface (Ethernet interface, aggregate interface, or SVI). When the function is enabled, the SNMP module sends link traps if the link status changes on the interface.

**Configuration Examples** The following example configures the interface not to send link traps.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

The following example configures the interface to send link traps.

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# snmp trap link-status
```

**Verifications** N/A

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.24 speed

Run this command to configure the speed of an interface.

**speed [ 10 | 100 | 1000 | 2500 | 5000 | 10G | auto ]**

Run this command to restore the default configuration.

**no speed**

**Parameter Description**

Parameter	Description
<b>10</b>	The interface speed of 10 Mbps.
<b>100</b>	The interface speed of 100 Mbps.
<b>1000</b>	The interface speed of 1000 Mbps.
<b>2500</b>	The interface speed of 2500 Mbps.
<b>5000</b>	The interface speed of 5000 Mbps.
<b>10G</b>	The interface speed of 10 Gbps.
<b>auto</b>	Indicates that the speed of the interface is adaptive.

**Defaults** The interface speed is adaptive by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** If an interface is an AP member port, the speed of this interface is determined by the speed of the AP. When the interface exits the AP, it uses its own speed configuration. You can run the **show interfaces** command to view the speed configuration. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of a small form-factor pluggable (SFP) interface to 10 Mbps.

**Configuration Examples** The following example sets the speed of the interface GigabitEthernet 0/1 to 100 Mbps.

```

Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# speed 100

```

**Verification** Run the **show interfaces** command to display the interface rate.



**Notifications**    N/A

**Common  
Errors**            N/A

**Platform  
Description**      N/A



# Ethernet Switching Commands

---

1. MAC Address Commands
2. VLAN Commands
3. LLDP Commands

# 1 MAC Address Commands

## 1.1 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

**clear mac-address-table dynamic** [ **address** *mac-address* [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] ] { [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] }

Parameter	Parameter	Description
Description	<b>dynamic</b>	Clears all the dynamic MAC addresses.
	<b>address</b> <i>mac-address</i>	Clears the specified dynamic MAC address.
	<b>interface</b> <i>interface-type interface-number</i>	Clears all the dynamic MAC addresses of the specified interface.
	<b>vlan</b> <i>vlan-id</i>	Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** Use the **show mac-address-table dynamic** command to display all the dynamic MAC addresses.

**Configuration** The following command clears all the dynamic MAC addresses.

**Examples**

```
Hostname# clear mac-address-table dynamic
```

Related	Command	Description
Commands	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address.

**Platform** N/A

**Description**

## 1.2 mac-address-table aging-time

Use this command to specify the aging time of the dynamic MAC address. Use the **no** or **default** form of the command to restore the default setting.

**mac-address-table aging-time** *seconds*

**no mac-address-table aging-time**

**default mac-address-table aging-time**

Parameter	Description
-----------	-------------

<b>Parameter Description</b>	<i>seconds</i>	Aging time of the dynamic MAC address in seconds. The value 0 indicates no aging.						
<b>Defaults</b>	The default is 300.							
<b>Command Mode</b>	Global configuration mode.							
<b>Usage Guide</b>	Use <b>show mac-address-table aging-time</b> to display configuration.							
<b>Configuration Examples</b>	The following example sets the aging time of the dynamic MAC address to 500 seconds.							
	<pre>Hostname(config)# mac-address-table aging-time 500</pre>							
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show mac-address-table aging-time</b></td> <td>Displays the aging time of the dynamic MAC address.</td> </tr> <tr> <td><b>show mac-address-table dynamic</b></td> <td>Displays dynamic MAC address.</td> </tr> </tbody> </table>	Command	Description	<b>show mac-address-table aging-time</b>	Displays the aging time of the dynamic MAC address.	<b>show mac-address-table dynamic</b>	Displays dynamic MAC address.	
Command	Description							
<b>show mac-address-table aging-time</b>	Displays the aging time of the dynamic MAC address.							
<b>show mac-address-table dynamic</b>	Displays dynamic MAC address.							
<b>Platform Description</b>	N/A							

### 1.3 mac-address-table filtering

Use this command to configure the filtering MAC address. Use the **no** or **default** form of the command to restore the default setting.

**mac-address-table filtering** *mac-address* **vlan** *vlan-id*

**no mac-address-table filtering** *mac-address* **vlan** *vlan-id*

**default mac-address-table filtering** *mac-address* **vlan** *vlan-id*

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>mac-address</i></td> <td>Filtering Address</td> </tr> <tr> <td><i>vlan-id</i></td> <td>VLAN ID, in the range from 1 to 4094.</td> </tr> </tbody> </table>	Parameter	Description	<i>mac-address</i>	Filtering Address	<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.
Parameter	Description						
<i>mac-address</i>	Filtering Address						
<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.						
<b>Defaults</b>	No filtering address is configured by default.						
<b>Command Mode</b>	Global configuration mode.						
<b>Usage Guide</b>	The filtering MAC address shall not be a multicast address.						
<b>Configuration Examples</b>	The following example configures the filtering MAC address for VLAN 1.						
	<pre>Hostname(config)# mac-address-table filtering 0000.0202.0303 vlan 3</pre>						

Related Commands	Command	Description
	<b>clear mac-address-table filtering</b>	Clears the filtering MAC address.

**Platform** N/A  
**Description**

## 1.4 mac-address-table static

Use this command to configure a static MAC address. Use the **no** or **default** form of the command to restore the default setting.

**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-type* *interface-number*  
**no mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-type* *interface-number*  
**default mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-type* *interface-number*

Parameter	Parameter	Description
<b>Description</b>	<i>mac-address</i>	Destination MAC address of the specified entry
	<i>vlan-id</i>	VLAN ID of the specified entry, in the range from 1 to 4094.
	<i>interface-type</i> <i>interface-number</i>	Interface (physical interface or aggregate port) that packets are forwarded to

**Defaults** No static MAC address is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use the **show mac-address-table static** command to display the static MAC address.

**Configuration Examples** N/A

Related Commands	Command	Description
	<b>show mac-address-table static</b>	Displays the static MAC address.

**Platform** N/A  
**Description**

## 1.5 show mac-address-learning

Use this command to display the MAC address learning.

**show mac-address-learning**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** All modes.

**Usage Guide** N/A

**Configuration Examples** The following example displays the MAC address learning.

**Examples**

```

Hostname# show mac-address-learning
GigabitEthernet 0/1      learning ability: disable
GigabitEthernet 0/2      learning ability: enable
  
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.6 show mac-address-table

Use this command to display all types of MAC addresses (including dynamic addresses, static addresses, filter addresses, and addresses of successfully authenticated users).

**show mac-address-table** [ **address** *mac-address* ] [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ]

Parameter	Parameter	Description
Description	<b>address</b> <i>mac-address</i>	The MAC address.
	<b>interface</b> <i>interface-type interface-number</i>	The Interface ID.
	<b>vlan</b> <i>vlan-id</i>	The VLAN ID, in the range from 1 to 4094.

**Defaults** N/A

**Command** All modes  
**Mode**

**Usage Guide** Type of the MAC address:

- type of the MAC address: e fr.
- type of the dynamic MAC address.
- type of the dynamic MAC address.
- OTHER: MAC address of a user authenticated via 802.1X, MAB, or Web-based authentication.

**Configuration** The following example displays the MAC address.

**Examples**

```

Hostname# show mac-address-table address 00d0.f800.1001
Vlan      MAC Address      Type      Interface
-----  -
1         00d0.f800.1001  STATIC   GigabitEthernet 0/1

Hostname# show mac-address-table
Vlan      MAC Address      Type      Interface
-----  -
1         00d0.f800.1001  STATIC   GigabitEthernet 0/1
1         00d0.f800.1002  DYNAMIC  GigabitEthernet 0/1
1         00d0.f800.1003  OTHER    GigabitEthernet 0/1
1         00d0.f800.1004  FILTER
    
```

Field	Description
Vlan	The interface address.
MAC Address	The MAC address.
Type	The MAC address type.
Interface	The interface corresponding to the MAC address.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.7 show mac-address-table aging-time

Use this command to display the aging time of the dynamic MAC address.

**show mac-address-table aging-time**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command** All modes  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the aging time of the dynamic MAC address.

**Examples**

```
Hostname# show mac-address-table aging-time
Aging time : 300
```

**Related  
 Commands**

Command	Description
<b>mac-address-table aging-time</b>	Sets the aging time of the dynamic MAC address.

**Platform** N/A  
**Description**

## 1.8 show mac-address-table count

Use this command to display the number of address entries in the address table.

**show mac-address-table count** [ **interface** *interface-type interface-number* | **vlan** *vlan-id* ]

**Parameter  
 Description**

Parameter	Description
<b>interface</b> <i>interface-type interface-number</i>	Interface ID
<b>vlan</b> <i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

**Defaults** N/A

**Command  
 Mode** Privileged EXEC mode.

**Usage Guide** The **show mac-address-table count** command is used to display the number of entries based on the type of MAC address entry.

The **show mac-address-table count interface** command is used to display the number of entries based on the interface associated with the MAC address entry.

The **show mac-address-table count vlan** command is used to display the number of entries based on the VLAN of MAC address entries.

**Configuration** The following example displays the number of MAC address entries.

**Examples**

```
Hostname# show mac-address-table count
Dynamic Address Count : 51
Static Address Count : 0
Filter Address Count : 0
Other Address Count : 0
```



```
Total Mac Addresses : 51
Total Mac Address Space Available: 8139
```

The following example displays the number of MAC address in VLAN 1.

```
Hostname# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Other Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 7
```

The following example displays the number of MAC addresses on interface g0/1.

```
Hostname# show mac-address-table interface gigabitEthernet 0/1
Dynamic Address Count : 10
Static Address Count : 0
Other Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 10
```

**Related  
Commands**

Command	Description
<b>show mac-address-table static</b>	Displays the static address.
<b>show mac-address-table filtering</b>	Displays the filtering address.
<b>show mac-address-table dynamic</b>	Displays the dynamic address.
<b>show mac-address-table address</b>	Displays all the address information of the specified address.
<b>show mac-address-table interface</b>	Displays all the address information of the specified interface.
<b>show mac-address-table vlan</b>	Displays all the address information of the specified vlan.

**Platform** N/A  
**Description**

## 1.9 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

```
show mac-address-table dynamic [ address mac-address ] [ interface interface-type interface-number ] [ vlan vlan-id ]
```

**Parameter  
Description**

Parameter	Description
<i>mac-address</i>	Destination MAC address of the entry
<i>vlan-id</i>	VLAN of the entry, in the range from 1 to 4094.
<i>interface-type interface-number</i>	Interface that the packet is forwarded to. It may be a physical port or an aggregate port

**Defaults****Command** All modes.**Mode****Usage Guide** N/A**Configuration** The following example displays the dynamic MAC address.**Examples**

```

Hostname# show mac-address-table dynamic
Vlan  MAC Address      Type  Interface
-----
1     0000.0000.0001      DYNAMIC  gigabitethernet 0/1
1     0001.960c.a740      DYNAMIC  gigabitethernet 0/1
1     0007.95c7.dff9      DYNAMIC  gigabitethernet 0/1
1     0007.95cf.eee0      DYNAMIC  gigabitethernet 0/1
1     0007.95cf.f41f      DYNAMIC  gigabitethernet 0/1
1     0009.b715.d400      DYNAMIC  gigabitethernet 0/1
1     0050.bade.63c4      DYNAMIC  gigabitethernet 0/1

```

**Related****Commands**

Command	Description
<b>clear mac-address-table dynamic</b>	Clears the dynamic MAC address.

**Platform** N/A**Description**

## 1.10 show mac-address-table filtering

Use this command to display the filtering MAC address.

**show mac-address-table filtering** [ **address** *mac-address* ] [ **vlan** *vlan-id* ]**Parameter****Description**

Parameter	Description
<i>mac-address</i>	Destination MAC address of the entry
<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094.

**Defaults** N/A**Command** Privileged EXEC mode.**Mode****Usage Guide** N/A**Configuration** The following example displays the filtering MAC address.**Examples**

```

Hostname# show mac-address-table filtering
Vlan  MAC Address      Type  Interface

```

```
-----
1    0000.2222.2222  FILTER Not available
```

Related Commands	Command	Description
	<b>mac-address-table filtering</b>	Configures the filtering MAC address.

**Platform** N/A  
**Description**

## 1.11 show mac-address-table interface

Use this command to display all the MAC addresses on the specified interface including static and dynamic MAC address

**show mac-address-table interface** [ *interface-type interface-number* ] [ **vlan** *vlan-id* ]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Displays the MAC address information of the specified Interface (physical interface or aggregate port).
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all the MAC addresses on interface gigabitethernet 0/1.

```
Hostname# show mac-address-table interface gigabitethernet 0/1
Vlan MAC Address Type Interface
-----
1    00d0.f800.1001 STATIC gigabitethernet 0/1
1    00d0.f800.1002 STATIC gigabitethernet 0/1
1    00d0.f800.1003 STATIC gigabitethernet 0/1
1    00d0.f800.1004 STATIC gigabitethernet 0/1
```

Related Commands	Command	Description
	<b>show mac-address-table static</b>	Displays the static MAC address.
	<b>show mac-address-table filtering</b>	Displays the filtering MAC address.
	<b>show mac-address-table dynamic</b>	Displays the dynamic MAC address.
	<b>show mac-address-table address</b>	Displays all types of MAC addresses.
	<b>show mac-address-table vlan</b>	Displays all types of MAC addresses of the specified VLAN.
	<b>show mac-address-table count</b>	Displays the address counts in the MAC address table.

**Platform** N/A  
**Description**

## 1.12 show mac-address-table static

Use this command to display the static MAC address.

**show mac-address-table static** [ **address** *mac-address* ] [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ]

Parameter	Parameter	Description
<b>Description</b>	<i>mac-address</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.
	<i>interface-type interface-number</i>	Interface of the entry physical interface or aggregate port

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays the static MAC addresses

### Examples

```

Hostname# show mac-address-table static
Vlan    MAC Address    Type    Interface
-----
1 00d0.f800.1001 STATIC gigabitethernet 0/1
1 00d0.f800.1002 STATIC gigabitethernet 0/1
1 00d0.f800.1003 STATIC gigabitethernet 0/1

```

Related	Command	Description
<b>Commands</b>	<b>mac-address-table static</b>	Configures the static MAC address.

**Platform** N/A  
**Description**

## 1.13 show mac-address-table vlan

Use this command to display all addresses of the specified VLAN.

**show mac-address-table vlan** [ *vlan-id* ]

Parameter	Parameter	Description
<b>Description</b>	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays all addresses of the specified VLAN.

**Examples**

```

Hostname# show mac-address-table vlan 1
Vlan  MAC Address      Type      Interface
-----
1      00d0.f800.1001      STATIC    gigabitethernet 0/1
1      00d0.f800.1002      STATIC    gigabitethernet 0/1
1      00d0.f800.1003      STATIC    gigabitethernet 0/1

```

**Related Commands**

Command	Description
<b>show mac-address-table static</b>	Displays static addresses.
<b>show mac-address-table filtering</b>	Displays filtered addresses.
<b>show mac-address-table dynamic</b>	Displays dynamic addresses.
<b>show mac-address-table address</b>	Displays all address information about the specified address.
<b>show mac-address-table interface</b>	Displays all address information about the specified interface.
<b>show mac-address-table count</b>	Displays the number of addresses in the address table.

**Platform Description** N/A

# 1 VLAN Commands

## 1.1 add interface

Run this command to add one access port or a group of access ports to the virtual local area network (VLAN).

**add interface** { *interface-type interface-number* | **range** *interface-type interface-range* }

Run this command to delete the current VLAN (other than VLAN 1) of one access port or a group of access ports to VLAN 1.

**no add interface** { *interface-type interface-number* | **range** *interface-type interface-range* }

Run this command to restore one access port or a group of access ports from the current VLAN.

**default add interface** { *interface-type interface-number* | **range** *interface-type interface-range* }

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Specifies an interface in format of <i>interface-type [ slot / ] int</i> . The values are L2 Ethernet interfaces or L2 aggregation ports (APs).
	<b>range</b> <i>interface-type interface-range</i>	Specifies a group of interfaces in format of <i>interface-type [ slot / ] intmin – intmax,int</i> . The values are L2 Ethernet interfaces or L2 APs.

**Defaults** All L2 Ethernet interfaces belong to VLAN 1 by default, and no port exists in new VLANs.

**Command mode** VLAN configuration mode

**Default Level** 14

**Usage Guide** This command takes effect to access ports only. If the interface is, for example, a trunk port, run the

**switchport trunk allowed vlan** { **add** *vlan-list* | **remove** *vlan-list* } command to modify the allowed VLANs list of the interface.

You must run the **interface aggregateport** *ap-number* command to create an AP before adding the AP to a VLAN. When you use this command to add an L2 AP to the current VLAN, the configuration takes effect to the L2 AP only.

**Configuration Examples**

The following example adds an access port GigabitEthernet 0/10 to VLAN 20 and displays the status and information about GigabitEthernet 0/10.

```

Hostname# configure terminal
Hostname (config)#vlan 20
Hostname (config-vlan)#add interface GigabitEthernet 0/10
Hostname (config-vlan)#show int g 0/10 sw

```

Interface	Switchport	Mode	Access	Native	Protected	VLAN lists
GigabitEthernet 0/10	enabled	ACCESS	20	1	Disabled	ALL

The following example adds a group of access ports to VLAN 200 and displays the member port information of the VLAN.

```

Hostname# configure terminal
Hostname (config)#vlan 200
Hostname (config-vlan)#add interface range GigabitEthernet 0/1-10
Hostname# show vlan
Hostname #show vlan

```

VLAN Name	Status	Ports
1 VLAN0001	STATIC	Gi0/11, Gi0/12, Gi0/13, Gi0/14 Gi0/15, Gi0/16, Gi0/17, Gi0/18 Gi0/19, Gi0/20, Gi0/21, Gi0/22 Gi0/23, Gi0/24
200 VLAN0200	STATIC	Gi0/1, Gi0/2, Gi0/3, Gi0/4 Gi0/5, Gi0/6, Gi0/7, Gi0/8 Gi0/9, Gi0/10

The following example adds AggregatePort 10 to VLAN 20 and displays the information about AggregatePort 10.

```

Hostname# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10
Hostname# show interface aggregateport 10 switchport

```

Interface	Switchport	Mode	Access	Native	Protected	VLAN lists
AggregatePort 10	enabled	ACCESS	20	1	Disabled	ALL

```
AggregatePort 10 enabled ACCESS 20 1 Disabled ALL
```

**Verifications** Run the **show vlan** command to check whether the port is successfully added to the VLAN.

**Notifications** N/A

**Common Errors** The interface to be added or deleted is not an L2 switch port.

The interface to be added or deleted is not an access port.

The interface to be added or deleted is a member port of the AP, or the AP is not created in advance.

**Platform Description** N/A

## 1.2 encapsulation

Run this command to configure an interface or sub-interface to tag packets with a specified VLAN ID.

**encapsulation dot1q *vlan-id***

Run this command to configure an interface or sub-interface not to tag packets with a specified VLAN ID.

**no encapsulation**

Run this command to restore the default configuration.

**default encapsulation**

**Parameter Description**

Parameter	Description
<i>vlan-id</i>	Specifies a VLAN ID for encapsulation. The value range is from 1 to 4,094.

**Defaults** By default, an interface or sub-interface does not tag packets with a specified VLAN ID.



**Command mode** Interface configuration mode

**Default Level** 14

**Usage Guide** After VLAN encapsulation is configured on an interface, the interface works in hybrid mode. The interface and all its sub-interfaces cannot tag packets with the same VLAN ID.

**Configuration Examples** 1. Configure the GigabitEthernet 0/1 to encapsulate VLAN 1 into packets.

```

Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#encapsulation dot1q 1
Hostname(config-if-GigabitEthernet 0/1)#exit
Hostname#show vlan
VLAN          Name                               Status    Ports
-----
          1 VLAN0001                    STATIC    Gi0/1
Hostname#show interface gigabitethernet 0/1
Index(dec):2 (hex):2
GigabitEthernet 0/2 is DOWN , line protocol is DOWN
  Hardware is BCM47622 GigabitEthernet, address is 00d0.f019.911b (bia 00d0.f019.911b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 1970-01-01 08:00:35
    Time duration since last link state change: 5 days,  4 hours, 13 minutes, 43 seconds
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
  Bridge attributes:
    Port-type: hybrid
    Tagged vlan id: none
    Untagged vlan id: 1
  Rxload is 1/255, Txload is 1/255
    10 seconds input rate 0 bits/sec, 0 packets/sec
    10 seconds output rate 0 bits/sec, 0 packets/sec

```

```

0 packets input, 0 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns, 0 no buffer, 0 dropped
0 output errors, 0 collisions, 0 interface resets

```

## 2. Configure the sub-interface, GigabitEthernet 0/1.1, to encapsulate VLAN 2 into packets.

```

Hostname(config)# vlan 2
Hostname(config-vlan)# exit
Hostname(config)# interface gigabitethernet 0/1.1
Hostname(config-subif-GigabitEthernet 0/1.1)# encapsulation dot1q 2
Hostname(config-subif-GigabitEthernet 0/1.1)# exit
Hostname#show vlan

```

VLAN	Name	Status	Ports
1	VLAN0001	STATIC	Gi0/1
2	VLAN0002	STATIC	Gi0/1.1

```

-----
Hostname#show interface gigabitethernet 0/1.1
ifindex(dec):8 (hex):8
GigabitEthernet 0/2.1 is DOWN , line protocol is DOWN
  Hardware is BCM47622 GigabitEthernet, address is 00d0.f019.911b (bia 00d0.f019.911b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is 802.1Q Virtual LAN, Vlan ID 2

```

**Verifications** Run the **show interface** command to display the encapsulation VLAN ID of an interface or a sub-interface. Run the **show vlan** command to display the interfaces added to a VLAN.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.3 interface bvi

Run this command to create a bridge virtual interface (BVI) for a VLAN and enter the BVI configuration mode.

**interface bvi** *bvi-id*

Run this command to delete a BVI from the VLAN.

**no interface bvi** *bvi-id*

Run this command to restore the default configuration.

**default interface bvi** *bvi-id*

Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID.

**Defaults** No BVI is configured for a VLAN by default.

**Command mode** Global configuration mode  
VLAN configuration mode  
Interface configuration mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example creates a BVI for VLAN 2 and configures the IP address of the BVI.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip address 10.10.29.1/24

```

- Verifications**
1. Run the **show interface description** command to display the created BVI.
  2. Run the **show interface vlan *vlan-id*** command to display the detailed configuration of the BVI.

**Notifications** N/A

**Platform Description** N/A

## 1.4 name

Use this command to specify the name of a VLAN. Use the **no** or **default** form of this command to restore the default setting.

**name** *vlan-name*

**no name**

**default name**

**Parameter Description**

Parameter	Description
<i>vlan-name</i>	VLAN name

**Defaults** The default name of a VLAN is the combination of “VLAN” and VLAN ID, for example, the default name of the VLAN 2 is “VLAN0002”.

**Command mode** VLAN configuration Mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the name of VLAN to vlan10.

```

Hostname(config)# vlan 10
Hostname(config-vlan)# name vlan10

```

**Related Commands**

Command	Description
<b>show vlan</b>	Displays member ports of the VLAN.

**Platform Description** N/A

## 1.5 show vlan

Use this command to display member ports of the VLAN.

**show vlan** [ id *vlan-id* ]

Parameter Description	Parameter	Description
	id <i>vlan-id</i>	VLAN ID

**Defaults** N/A

**Command mode** All modes

**Usage Guide** N/A

**Configuration** The following command displays the status of VLAN 1.

**Examples**

```

Hostname(config-vlan)#show vlan id 20
VLAN Name                Status    Ports
-----
 20 VLAN0020              STATIC    Gi0/1
  
```

The following command displays the status of all VLANs.

```

Hostname(config-vlan)#show vlan
VLAN Name                Status    Ports
-----
 1 VLAN0001              STATIC    Gi0/1
 2 VLAN0002              STATIC
20 VLAN0020              STATIC
  
```

Output Fields of the show vlan Command:

Field	Description
VLAN	VLAN ID
Name	VLAN name
Status	Attribute of a VLAN <ul style="list-style-type: none"> <li>● <b>STATIC:</b> static VLAN</li> <li>● <b>Dynamic:</b> dynamic VLAN</li> <li>● <b>PRIVATE:</b> primary or secondary VLAN of a private VLAN</li> <li>● <b>SUPER:</b> super VLAN</li> <li>● <b>SUB:</b> sub VLAN of a super VLAN</li> </ul>

<b>Related Commands</b>	Ports	Ports that are added to this VLAN
	Command	Description
	<b>name</b>	VLAN name.

**Platform** N/A  
**Description**

## 1.6 vlan

Use this command to enter the VLAN configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**vlan** { *vlan-id* | **range** *vlan-range* }

**no vlan** { *vlan-id* | **range** *vlan-range* }

**default vlan** { *vlan-id* | **range** *vlan-range* }

<b>Parameter Description</b>	Parameter	Description
	<i>vlan-id</i>	VLAN ID Default VLAN (VLAN 1) cannot be removed.
	<b>range</b> <i>vlan-range</i>	VLAN ID range.

**Defaults** The default is static VLAN.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example creates VLAN 10.

```

Hostname(config)# vlan 10
Hostname(config-vlan)#
    
```

<b>Related Commands</b>	Command	Description
	<b>show vlan</b>	Displays member ports of the VLAN.

**Platform** N/A  
**Description**

# 1 LLDP Commands

## 1.1 civic-location

Use this command to configure a common LLDP address.

```
{ country | state | county | city | division | neighborhood | street-group | leading-
street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix |
landmark | additional-location-information | name | postal-code | building | unit | floor
| room | type-of-place | postal-community-name | post-office-box | additional-code }
ca-word
```

Run the **no** form of this command to remove this configuration.

```
no { country | state | county | city | division | neighborhood | street-group | leading-
street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix |
landmark | additional-location-information | name | postal-code | building | unit | floor
| room | type-of-place | postal-community-name | post-office-box | additional-code }
ca-word
```

Parameter  
Description

Parameter	Description
<b>country</b>	Country code, two bytes.
<b>state</b>	state, Address information, the CA type is 1
<b>county</b>	county, the CA type is 2
<b>city</b>	city, the CA type is 3
<b>division</b>	district, the CA type is 4
<b>neighborhood</b>	community, the CA type is 5
<b>street-group</b>	street, the CA type is 6
<b>leading-street-dir</b>	street No., the CA type is 16
<b>trailing-street-suffix</b>	street No., the CA type is 17
<b>street-suffix</b>	street No., the CA type is 18
<b>number</b>	street No., the CA type is 19
<b>street-number-suffix</b>	street No., the CA type is 20
<b>landmark</b>	landmark, the CA type is 21
<b>additional-location-information</b>	additional address, the CA type is 22
<b>name</b>	name, the CA type is 23
<b>postal-code</b>	postal code, the CA type is 24
<b>building</b>	building, the CA type is 25
<b>unit</b>	unit, the CA type is 26
<b>floor</b>	floor, the CA type is 27
<b>room</b>	room, the CA type is 28
<b>type-of-place</b>	place type, the CA type is 29

<b>postal-community-name</b>	post office, the CA type is 30
<b>post-office-box</b>	post office box, the CA type is 31
<b>additional-code</b>	additional code, the CA type is 32
<i>ca-word</i>	Address information. When the address type is <b>country</b> , only two characters can be used to represent a country.

**Defaults** No address information is configured by default.

**Command Mode** LLDP Civic address configuration mode

**Usage Guide** This command is used to configure a common LLDP address in LLDP Civic address configuration mode.  
 Run the **show lldp location civic-location { identifier *id* | interface *interface-type interface-number* | static }** command to display the information about the common LLDP address. If no common LLDP address is configured, no address type or information will be displayed.

**Configuration** The following example configures an LLDP Civic Address (ID: 1).

**Examples**

```

Hostname#config
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# country CH
Hostname(config-lldp-civic)# city Fuzhou
    
```

Related Commands	Command	Description
	<b>show lldp location civic-location { identifier <i>id</i>   interface <i>interface-type interface-number</i>   static }</b>	Displays the information about an LLDP Civic address.

**Platform Description** N/A

## 1.2 clear lldp statistics

Use this command to clear LLDP statistics.

**clear lldp statistics [ interface *interface-type interface-number* ]**

Parameter	Parameter	Description
<b>Description</b>	<b>interface <i>interface-type interface-number</i></b>	Clears the LLDP statistics of the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode



**Usage Guide** When the **interface** parameter is specified, this command will clear the LLDP statistics of the specified interface.

**Configuration** The following example clears LLDP statistics of interface 1.

**Examples**

```

Hostname# clear lldp statistics interface GigabitEthernet 0/1
Hostname# show lldp statistics interface GigabitEthernet 0/1
Lldp statistics information of port [GigabitEthernet 0/1]
-----
The number of lldp frames transmitted : 0
The number of frames discarded : 0
The number of error frames : 0
The number of lldp frames received : 0
The number of TLVs discarded : 0
The number of TLVs unrecognized : 0
The number of neighbor information aged out : 0
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.3 clear lldp table

Use this command to clear LLDP neighbor information.

**clear lldp table [ interface interface-type interface-number ]**

Parameter	Parameter	Description
<b>Description</b>	<b>interface interface-type interface-number</b>	The LLDP neighbor information on the specified interface is cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the **interface interface-type interface-number** parameter is specified, the LLDP neighbor information on the specified interface is cleared.  
 If the **interface interface-type interface-number** parameter is not specified, the LLDP neighbor information on all interfaces is cleared.

**Configuration** The following example clears the LLDP neighbor information on interface 1.

**Examples**

```

Hostname# show lldp neighbors interface GigabitEthernet 0/1
Capability codes:
    
```

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
System Name          Local Intf      Port ID
Capability  Aging-time

Total entries displayed: 0
Hostname# clear lldp table interface GigabitEthernet 0/1
Hostname# show lldp neighbors interface GigabitEthernet 0/1
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.4 device-type

Use this command to configure the device type.

**device-type** *device-type*

Run this command to remove this configuration.

**no device-type**

Parameter Description	Parameter	Description
	<i>device-type</i>	Device type. The value ranges from 0 to 2. <ul style="list-style-type: none"> <li>● 0: The device type is DHCP Server.</li> <li>● 1: The device type is switch.</li> <li>● 2: The device type is LLDP MED terminal.</li> </ul>

**Defaults** By default, the device type is 1, that is, switch.

**Command Mode** LLDP Civic address configuration mode

**Usage Guide** This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.  
 Run the **show lldp location civic-location { identifier *id* | interface *interface-type interface-number* | static }** command to display the device type. The default device type information is not displayed.

**Configuration Examples** 1 The following example sets the device type to switch.

```
Hostname#config terminal
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# device-type 1
```

Related Commands	Command	Description
	<b>show lldp location civic-location</b> { identifier <i>id</i>   interface <i>interface-type interface-number</i>   static }	Displays LLDP civic address information.

**Platform** N/A  
**Description**

## 1.5 lldp enable

Use this command to enable the LLDP globally or on the interface. Use **no** form of this command to disable this function.

**lldp enable**  
**no lldp enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The LLDP function is enabled by default.

**Command Mode** Global configuration mode/Interface configuration mode

**Usage Guide** LLDP takes effect on an interface only when LLDP is enabled globally.

**Configuration Examples** The following example disables LLDP globally and on the interface.

```

Hostname#config
Hostname(config)#no lldp enable
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)# no lldp enable

```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.6 lldp encapsulation snap

Run this command to set the LLDP packet encapsulation format to Subnetwork Access Protocol (SNAP).

**lldp encapsulation snap**

Run this command to restore the default configuration.


**no lldp encapsulation snap**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The default LLDP packet encapsulation format is Ethernet II.

**Command** Interface configuration mode.

**Mode**

**Usage Guide**  To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.

**Configuration** The following example sets LLDP packet encapsulation format to SNAP.

**Examples**

```

Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp encapsulation snap

```

Related	Command	Description
Commands	<b>show lldp status</b>	Displays LLDP status information.

**Platform** N/A

**Description**

## 1.7 lldp error-detect

Run this command to enable the LLDP error detection function.

**lldp error-detect**

Run the **no** form of this command to disable this feature.

**no lldp error-detect**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The LLDP error detection function is enabled by default.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** LLDP error detection function includes detecting the VLAN configuration at both ends of a link, interface status, aggregate port configuration, MTU configuration, and loops. When LLDP detects an error, an alarm is generated to alert administrators.

LLDP error detection relies on the specific TLV in the LLDP packets exchanged between devices on both sides of the link. To ensure normal functioning of the detection feature, correct TLVs must be advertised.

**Configuration** The following example configures LLDP error detection.

**Examples**

```

Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp error-detect

```

**Related  
Commands**

Command	Description
<b>show interface status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.8 lldp fast-count

Run this command to configure the number of LLDP packets that can be transmitted rapidly.

**lldp fast-count** *fast-count-value*

Run this command to remove this configuration.

**no lldp fast-count**

**Parameter  
Description**

Parameter	Description
<i>fast-count-value</i>	The number of fast sent LLDP packets, in the range from 1 to 10.

**Defaults** The default is 3.

**Command  
Mode** Global configuration mode.

**Usage Guide** When LLDP discovers a new neighbor or the LLDP work mode is changed from disabled or Rx to TxRx or Tx, the fast transmission mechanism is started so that the neighbor quickly learns the information of the device. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval.

**Configuration** The following example sets the number of fast sent LLDP packets to 5.

**Examples**

```

Hostname# config
Hostname(config)# lldp fast-count 5

```

Related	Command	Description
Commands	<b>show interface status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.9 Ildp hold-multiplier

Use this command to set the TTL multiplier.

**Ildp hold-multiplier** *tvl-value*

Run this command to remove this configuration

**no Ildp hold-multiplier**

Parameter	Parameter	Description
Description	<i>tvl-value</i>	TTL multiplier, in the range from 2 to 10.

**Defaults** The default TTL multiplier of LLDP packets is 4.

**Command** Global configuration mode.  
**Mode**

**Usage Guide** The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.

**Configuration** The following example sets TTL multiplier to 5.

**Examples**

```

Hostname#config
Hostname(config)#lldp hold-multiplier 5

```

Related	Command	Description
Commands	<b>show Ildp status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.10 Ildp ignore pvid-error-detect

Use this command to enable the function of ignoring PVID function. Use the **no** form of this command to disable the function of ignoring PVID function.

**Ildp ignore pvid-error-detect**

**no Ildp ignore pvid-error-detect**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The function of ignoring PVID detection is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example ignores PVID detection globally.	
	<pre> Hostname# configure terminal Hostname(config)# lldp ignore pvid-error-detect </pre>	
Platform	N/A	
Description		

## 1.11 lldp location civic-location identifier

Run this command to configure the civic address in LLDP-MED TLVs.

Run this command to remove this configuration.

**lldp location civic-location identifier *id***

**no lldp location civic-location identifier *id***

Parameter	Parameter	Description
Description	<i>id</i>	Identifier of a civic address for a network device. The value range is from 1 to 1024.
Defaults	The common address of a device is not configured by default.	
Command Mode	Global configuration mode	
Usage Guide	This command can be used to enter the LLDP Civic Address configuration mode.	
Configuration Examples	The following example creates the Civic Address information in LLDP MED-TLV as follows: set <i>id</i> to 1.	
	<pre> Hostname#config Hostname(config)#lldp location civic-location identifier 1 Hostname(config-lldp-civic)# </pre>	

Related	Command	Description
Commands	<b>show lldp location civic-location</b> { identifier <i>id</i>   interface <i>interface-type interface-number</i>   static }	Displays the LLDP Civic Address information.

Platform N/A

Description

## 1.12 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Run the **no** form of this command to remove this configuration.

**lldp location elin identifier** *id elin-location tel-number*

**no lldp location elin identifier** *id*

Parameter	Parameter	Description
Description	<i>id</i>	ID of an emergency number, in the range from 1 to 1024.
	<b>elin-location</b> <i>tel-number</i>	Emergency number, in the range from 10 to 25 bytes.

**Defaults** The emergency telephone number of a device is not configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to configure an emergency number.

**Configuration** The following example sets an emergency number.

**Examples**

```

Hostname#config
Hostname(config)#lldp location elin identifier 1 elin-location
085283671111

```

Related	Command	Description
Commands	<b>show lldp location elin-location</b> { identifier <i>id</i>   interface <i>interface-type interface-number</i>   static }	Displays an LLDP emergency number.

Platform N/A

Description



## 1.13 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Run the **no** form of this command to remove this configuration.

**lldp management-address-tlv** *ip-address*

**no lldp management-address-tlv**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Management address to be advertised in an LLDP packet.

**Defaults** By default, the management address to be advertised in an LLDP packet is the IPv4 address of the minimum VLAN supported by the interface. If no IPv4 address is configured for the VLAN with the minimum ID, LLDP keeps searching the other VLANs with the minimum ID until a qualified IPv4 address is obtained. If no IPv4 address is found, LLDP searches the IPv6 address of the minimum VLAN supported by the interface. If no IPv6 address is found, the local address 127.0.0.1 is used as the management address to be advertised.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```

Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp management-address-tlv 192.168.1.1

```

Related Commands	Command	Description
	<b>show lldp local-information</b>	Displays LLDP local information

**Platform** N/A

**Description**

## 1.14 lldp mode

Use this command to configure the LLDP operating mode. Run the **no** form of this command to remove this configuration.

**lldp mode** { *rx* | *tx* | *txrx* }

**no lldp mode**

Parameter	Parameter	Description
Description	<i>rx</i>	Only sends LLDPDUs.

<b>tx</b>	Only receives LLDPDUs.
<b>txrx</b>	Sends and receives LLDPDUs.

**Defaults** The default LLDP work mode is **TxRx**, that is, an interface transmits and receives LLDPDUs.

**Command Mode** Interface configuration mode

**Usage Guide** Disable LLDP operating mode on the interface. The interface won't send and receive LLDP packets. The precondition for enabling LLDP on the interface is that LLDP has been enabled globally and LLDP operates in tx, rx or txrx mode.

**Configuration Examples** The following example sets LLDP operating mode to tx on the interface.

```

Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp mode tx

```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information

**Platform Description** N/A

## 1.15 lldp network-policy profile

Use this command to create an LLDP Network Policy and enter the LLDP Network Policy configuration mode. Run the **no** form of this command to remove this configuration.

**lldp network-policy profile** *profile-num*  
**no lldp network-policy profile** *profile-num*

Parameter Description	Parameter	Description
	<i>profile-num</i>	ID of an LLDP Network Policy, in the range from 1 to 1024.

**Defaults** No LLDP Network Policy is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enter the LLDP Network Policy configuration mode. When this command is run, the policy ID must be specified. In LLDP Network-Policy mode, the { **voice** | **voice-signaling** } **vlan** command can be used to configure the specific Network Policy.

**Configuration** The following example creates an LLDP Network Policy whose ID is 1.

**Examples**

```

Hostname#config
Hostname(config)#lldp network-policy profile 1
Hostname(config-lldp-network-policy)#

```

**Related**

**Commands**

Command	Description
<b>show lldp network-policy profile</b> [ <i>profile-num</i> ]	Displays an LLDP network policy.

**Platform**

N/A

**Description**

## 1.16 lldp notification remote-change enable

Use this command to configure LLDP trap function. Run the **no** form of this command to disable this feature.

**lldp notification remote-change enable**

**no lldp notification remote-change enable**

**Parameter**

**Description**

Parameter	Description
N/A	N/A

**Defaults**

The LLDP trap function is disabled by default.

**Command**

Interface configuration mode.

**Mode**

**Usage Guide**

By configuring LLDP trap function, the LLDP information of local device (such as information about the detection of new neighbor or the fault on the communication link) can be sent to the network management server. The administrator can monitor the network operation status according to such information.

**Configuration** The following example configures LLDP trap function.

**Examples**

```

Hostname#config
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if)#lldp notification remote-change enable

```

**Related**

**Commands**

Command	Description
<b>show lldp status</b>	Displays LLDP status information.

**Platform**

N/A

**Description**

## 1.17 lldp timer notification-interval

Run this command to configure the LLDP trap transmission interval.

Run this command to remove this configuration.

**lldp timer notification-interval** *trap*

**no lldp timer notification-interval**

Parameter	Parameter	Description
Description	<i>trap</i>	LLDP trap transmission interval, in seconds. The value range is from 5 to 3600.

**Defaults** The default LLDP trap transmission interval is 5 seconds.

**Command Mode** Global configuration mode.

**Usage Guide** You can configure an LLDP trap transmission interval to prevent frequent transmission of LLDP trap messages. LLDP information change is detected during this interval, traps will be sent to the network management server.

**Configuration Examples** The following example sets the LLDP trap transmission interval to 10 seconds.

```

Hostname# config
Hostname(config)# lldp timer notification-interval 10
    
```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

**Platform Description** N/A

## 1.18 lldp timer reinit-delay

Use this command to set port initialization delay. Run the **no** form of this command to remove this configuration.

**lldp timer reinit-delay** *reinit-delay*

**no lldp timer reinit-delay**

Parameter	Parameter	Description
Description	<i>reinit-delay</i>	Port initialization delay, in the range from 1 to 10 in the unit of seconds.

**Defaults** The default LLDP interface initialization delay is **2** seconds.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.

**Configuration Examples** The following example sets LLDP port initialization delay to 3 seconds.

```
Hostname#config
Hostname(config)#lldp timer reinit-delay 3
```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

**Platform Description** N/A

## 1.19 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Run the **no** form of this command to remove this configuration.

**lldp timer tx-delay** *tx-delay*  
**no lldp timer tx-delay**

Parameter Description	Parameter	Description
	<i>tx-delay</i>	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.

**Defaults** The default LLDP packet transmission delay is **2** seconds.

**Command Mode** Global configuration mode.

**Usage Guide** An LLDP-enabled port will send LLDP packets when the local device information changes. To avoid frequently sending LLDP packets due to the frequent local device information change, configure the LLDP packet transmission delay to control the frequent transmission of LLDP packets.

**Configuration Examples** The following example sets LLDPDU transmission delay to 3 seconds.

```
Hostname#config
Hostname(config)#lldp timer tx-delay 3
```

Related Commands	Command	Description
	<b>show lldp status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.20 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Run the **no** form of this command to remove this configuration.

**lldp timer tx-interval** *tx-interval*

**no lldp timer tx-interval**

Parameter	Parameter	Description
<b>Description</b>	<i>tx-interval</i>	Interval of sending the LLDP packets, in the range from 1 to 32768 in the unit of seconds.

**Defaults** The default LLDP packet transmission interval is **30** seconds.

**Command** Global configuration mode.  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the interval of sending the LLDP packets to 10 seconds.

### Examples

```
Hostname#config
Hostname(config)#lldp timer tx-interval 10
```

Related	Command	Description
<b>Commands</b>	<b>show lldp status</b>	Displays LLDP status information.

**Platform** N/A  
**Description**

## 1.21 lldp tlv-enable basic-tlv

Use this command to configure the optional basic management TLVs to be advertised.

Use the **no** form of this command to cancel the optional basic management TLVs to be advertised.

**lldp tlv-enable basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }

**no lldp tlv-enable basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }

Parameter	Description
-----------	-------------

<b>Parameter</b>	<b>all</b>	All optional basic management TLVs
<b>Description</b>	<b>port-description</b>	Port Description TLV
	<b>system-capability</b>	System Capabilities TLV
	<b>system-description</b>	System Description TLV
	<b>system-name</b>	System Name TLV

**Defaults** All optional basic management TLVs can be advertised on an interface.

**Command** Interface configuration mode

**Mode**

**Usage Guide** The following table lists basic management TLVs - a collection of basic TLVs used for network management.

TLV Type	TLV Description	Usage in LLDPDU
Chassis ID TLV	Identifies a device ID with a MAC address.	Mandatory
Port ID TLV	Identifies an interface sending an LLDPDU.	Mandatory
Time To Live TLV	TTL of local information on a neighbor. When a device receives a TLV with the TTL of 0, it deletes the neighbor information.	Mandatory
Port Description TLV	Description of the interface sending an LLDPDU.	Optional
System Name TLV	Device name.	Optional
System Description TLV	Device description, including the hardware version, software version, and operating system.	Optional
System Capabilities TLV	Main functions supported by the device, such as the bridge, routing, and relay functions.	Optional
Management Address TLV	Management address, which contains the interface ID and object identifier (OID).	Optional
End Of LLDPDU TLV	End flag of an LLDPDU, occupying two bytes.	Mandatory

This collection consists of two types of TLVs: mandatory TLVs and optional TLVs.

- Mandatory TLVs must be included in LLDPDUs for advertisement, and cannot be modified to the unadvertisable state by this command.
- In the device, an LLDPDU contains the management address TLV of optional TLVs to be advertised by default. This command does not affect the advertisement status and content of the management address TLV. You can run the **lldp management-address-tlv** command to configure the advertisement content of the management address TLV.
- You can run this command to configure whether to encapsulate the port description TLV, system name TLV, system description TLV, and system capabilities TLV of optional TLVs into LLDPDUs to be advertised.

**Configuration Examples** The following example configures all optional basic management TLVs to be advertised.

```

Hostname# configure terminal
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp tlv-enable basic-tlv all

```

Related Commands	Command	Description
	<b>show lldp tlv-config interface</b>	Displays the attributes of advertisable TLVs

**Platform** N/A

**Description**

## 1.22 lldp tlv-enable dot1-tlv

Use this command to configure the 802.1 organizationally specific TLVs to be advertised.

Use the **no** form of this command to cancel the 802.1 organizationally specific TLVs to be advertised.

**lldp tlv-enable dot1-tlv { all | port-vlan-id | protocol-vlan-id [ *vlan-id* ] | vlan-name [ *vlan-id* ] }**

**no lldp tlv-enable dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name }**

Parameter Description	Parameter	Description
	<b>all</b>	The Port VLAN ID TLV, the Port and Protocol VLAN ID TLV and the VLAN Name TLV
	<b>port-vlan-id</b>	Port VLAN ID TLV
	<b>protocol-vlan-id [ <i>vlan-id</i> ]</b>	Port and Protocol VLAN ID TLV
	<b>vlan-name [ <i>vlan-id</i> ]</b>	VLAN Name TLV. VLAN ID corresponding to the specified VLAN name

**Defaults** The Port VLAN ID TLV, the Port and Protocol VLAN ID TLV and the VLAN Name TLV can be advertised on an interface.

**Command Mode** Interface configuration mode

**Usage Guide** The IEEE 802.1 organizationally specific TLVs are listed in the following table. All TLV types are optional. You can run this command to configure whether to encapsulate the port VLAN ID TLV, port and protocol VLAN ID TLV, and VLAN name TLV into LLDPDUs to be advertised. The LLDP protocol used by this device does not allow the device to send a protocol identity TLV but the device can receive a protocol identity LV.

You can run the **show lldp tlv-config [ interface *interface-type interface-number* ]** command to display the advertisement status of optional TLVs on an interface. The STATUS field indicates the advertisement status and the DEFAULT field indicates the default advertisement status.

TLV Type	Description
Port VLAN ID TLV	Virtual local area network (VLAN) identifier of interface.
Port And Protocol VLAN ID TLV	Protocol VLAN identifier of an interface.
VLAN Name TLV	VLAN name of an interface.



Protocol Identity TLV	Protocol type supported by an interface.
-----------------------	--

**Configuration Examples** The following example configures all IEEE 802.1 TLVs to be advertised.

```

Hostname# configure terminal
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all
    
```

Related Commands	Command	Description
	<b>show lldp tlv-config interface</b>	Displays the attributes of advertisable TLVs

**Platform** N/A  
**Description**

### 1.23 lldp tlv-enable dot3-tlv

Use this command to configure the 802.3 organizationally specific TLVs to be advertised. Use the **no** form of this command to cancel the 802.3 organizationally specific TLVs to be advertised.

```

lldp tlv-enable dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power }
no lldp tlv-enable dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power }
    
```

Parameter	Parameter	Description
<b>Description</b>	<b>all</b>	All the IEEE 802.3 organizationally specific TLVs
	<b>link-aggregation</b>	Link Aggregation TLV
	<b>mac-physic</b>	MAC/PHY Configuration/Status TLV
	<b>max-frame-size</b>	Maximum Frame Size TLV
	<b>power</b>	Power via MDI TLV

**Defaults** All the IEEE 802.3 organizationally specific TLVs can be advertised on an interface.

**Command Mode** Interface configuration mode

**Usage Guide** The IEEE 802.1 organizationally specific TLVs are described in the following table. All TLV types are optional. You can run this command to configure whether to encapsulate them into an LLDPDU to be advertised.

You can run the **show lldp tlv-config [ interface interface-type interface-number ]** command to display the advertisement status of optional TLVs on an interface. The STATUS field indicates the advertisement status and the DEFAULT filed indicates the default advertisement status.

Link Aggregation TLV	Link aggregation capacity of an interface and aggregation state.
MAC/PHY Configuration/Status TLV	Rate and duplex mode of an interface, and whether an negotiation is supported and enabled.
Maximum Frame Size TLV	Maximum size of the frame that can be transmitted by interface.

Power Via MDI TLV	Power supply capacity of an interface.
Link Aggregation TLV	Link aggregation capacity of an interface and the aggregation state.

Follow the steps to allow an interface to advertise TLVs:

- (1) Allow the interface to advertise LLDP 802.3 MAC/PHY Configuration/Status TLVs;
- (2) Allow the interface to advertise LLDP-MED Capabilities TLVs.
- (3) Allow the interface to advertise other types of LLDP-MED TLVs except for Network Policy TLVs.

Follow the steps to disable the interface from advertising TLVs:

- (1) Disable the interface from advertising other types of LLDP-MED TLVs except for Network Policy TLVs.
- (2) Disable the interface from advertising LLDP-MED Capabilities TLVs.
- (3) Disable the interface from advertising LLDP 802.3 MAC/PHY Configuration/Status TLVs.

**Configuration Examples** The following example disables the GigabitEthernet 0/1 to advertise any IEEE 802.1 organizationally specific TLV.

```

Hostname# configure terminal
Hostname(config)#interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no lldp tlv-enable dot3-tlv all
    
```

Related Commands	Command	Description
	<b>show lldp tlv-config interface</b>	Displays the attributes of advertisable TLVs

**Platform** N/A  
**Description**

## 1.24 lldp tlv-enable med-tlv

Use this command to configure the LLDP MED TLVs to be advertised.

Use the **no** form of this command to cancel the LLDP MED TLVs to be advertised.

**lldp tlv-enable med-tlv { all | capability | inventory | location civic-location identifier *id* | location elin identifier *id* | network-policy profile [ *profile-num* ] | power-over-ethernet }**

**no lldp tlv-enable med-tlv { all | capability | inventory | location civic-location identifier *id* | location elin identifier *id* | network-policy profile [ *profile-num* ] | power-over-ethernet }**

Parameter Description	Parameter	Description
	<b>all</b>	All LLDP-MED TLVs except Location Identification TLVs
	<b>capability</b>	LLDP-MED Capabilities TLV
	<b>inventory</b>	Inventory management TLVs, including hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial

	number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.
<b>location civic-location identifier</b> <i>id</i>	Common address information about the network device in location identification TLVs. The policy ID ranges 1-1024.
<b>location elin identifier</b> <i>id</i>	Emergency number in location identification TLVs. The policy ID ranges from 1 to 1024.
<b>network-policy profile</b> [ <i>profile-num</i> ]	Network Policy TLV. The network policy ID ranges from 1 to 1024.
<b>power-over-ethernet</b>	Extended Power-via-MDI TLV

**Defaults** All types of LLDP-MED TLVs except the Location Identification TLV can be advertised on an interface.

**Command** Interface configuration mode

**Mode**

**Usage Guide** Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an extension to LLDP based on IEEE 802.1AB LLDP. It enables users to conveniently deploy the Voice over IP (VoIP) network and detect faults. LLDP-MED provides functions including the network configuration policies, device discovery, Power over Ethernet (PoE) management, and inventory management, to meet the requirements of low cost, effective management, and easy deployment and simplify the deployment of audio devices.

The LLDP-MED organizationally specific TLVs are listed in the following table. All TLV types are optional. You can run this command to configure whether to encapsulate them into an LLDPDU to be advertised.

You can run the **show lldp tlv-config [ interface interface-type interface-number ]** command to display the advertisement status of optional TLVs on an interface. The STATUS field indicates the advertisement status and the DEFAULT filed indicates the default advertisement status.

TLV Type	Description
Capabilities TLV	Whether the device supports LLDP-MED, the type of the LLDP-MED TLV encapsulated into an LLDPDU, and device type (the type of a network device or terminal).
Network Policy TLV	Interface VLAN configuration, supported application type (such as voice or video services), and Layer 2 priority.
Location Identification TLV	Contains the city location, including the common address and device type, and emergency phone number, used for the precise location of a device in applications such as network topology collection.
Extended Power-via-MDI TLV	Power options.
Inventory – Hardware Revision TLV	Hardware version of a MED device.
Inventory – Firmware Revision TLV	Firmware version of a MED device.
Inventory – Software Revision TLV	Software version of a MED device.
Inventory – Serial Number TLV	Serial number of a MED device.
Inventory – Manufacturer Name TLV	Name of the manufacturer of a MED device.
Inventory – Model Name TLV	Module name of a MED device.
Inventory – Asset ID TLV	Asset identifier of a MED device, used for inventory management and asset tracking.

Follow the steps to allow an interface to advertise TLVs:

- (1) Allow the interface to advertise LLDP 802.3 MAC/PHY Configuration/Status TLV.
- (2) Allow the interface to advertise LLDP-MED Capabilities TLV.
- (3) Allow the interface to advertise other types of LLDP-MED TLVs except for Network Policy TLVs.

Follow the steps to disable the interface from advertising TLVs:

- (1) Disable the interface from advertising other types of LLDP-MED TLVs except for Network Policy TLVs.
- (2) Disable the interface from advertising LLDP-MED Capabilities TLVs.
- (3) Disable the interface from advertising LLDP 802.3 MAC/PHY Configuration/Status TLVs.

**Configuration Examples** The following example configures the GigabitEthernet 0/1 to advertise the city location information.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location civic-location identifier 1
Hostname(config-lldp-civic)# country CH
Hostname(config-lldp-civic)# city A
Hostname(config-lldp-civic)# device-type 1
Hostname(config-lldp-civic)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable dot3-tlv mac-physic
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv capability
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv location civic-
location identifier 1

```

The following example configures the GigabitEthernet 0/1 to advertise the emergency number.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# lldp location elin identifier 1 elin-location 085283671111
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable dot3-tlv mac-physic
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv capability
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv location elin
identifier 1

```

The following example configures the GigabitEthernet 0/1 to advertise the network policy TLV 1.

```

Hostname> enable
Hostname# configure terminal
Hostname (config)# lldp network-policy profile 1
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 cos 4

```

```

Hostname(config-lldp-network-policy)# voice-signaling vlan 3 dscp 40
Hostname (config-lldp-network-policy)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable dot3-tlv mac-physic
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv capability
Hostname(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy
profile 1
    
```

Related	Command	Description
Commands	<b>show lldp tlv-config interface</b>	Displays the attributes of advertisable TLVs

**Platform** N/A  
**Description**

### 1.25 show lldp local-information

Use this command to display the LLDP information of local device. The information will be encapsulated in the TLVs and sent to the neighbor device.

**show lldp local-information [ global | interface *interface-type interface-number* ]**

Parameter	Parameter	Description
Description	<b>global</b>	Displays the global LLDP information to be sent.
	<b>interface <i>interface-type interface-number</i></b>	Displays the LLDP information of the specified interface to be sent.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** If no parameter is specified, all LLDP information is displayed, including global and interface-based LLDP information.

**Configuration Examples** The following example displays the device information to be sent to neighbor device.

```

Hostname# show lldp local-information
Global LLDP local-information:
Chassis ID type      : MAC address
Chassis id          : 00d0.f822.33aa
System name         : System name
System description  : System description
System capabilities supported : Repeater, Bridge, Router
System capabilities enabled  : Repeater, Bridge, Router
    
```

```
LLDP-MED capabilities      : LLDP-MED Capabilities, Network Policy, Location
    Identification, Extended Power via MDI-PD, Inventory
Device class              : Network Connectivity
HardwareRev               : 1.0
FirmwareRev               :
SoftwareRev               : RGOS 10.4(3) Release(94786)
SerialNum                 : 1234942570001
Manufacturer name         : Manufacturer name
Asset tracking identifier   :
-----
Lldp local-information of port [GigabitEthernet 0/1]
-----
Port ID type              : Interface name
Port id                   : GigabitEthernet 0/1
Port description          :

Management address subtype : 802 mac address
Management address        : 00d0.f822.33aa
Interface numbering subtype :
Interface number          : 0
Object identifier         :

802.1 organizationally information
Port VLAN ID              : 1
Port and protocol VLAN ID (PPVID) : 1
    PPVID Supported       : YES
    PPVID Enabled         : NO
VLAN name of VLAN 1      : VLAN0001
Protocol Identity         :

802.3 organizationally information
Auto-negotiation supported : YES
Auto-negotiation enabled  : YES
PMD auto-negotiation advertised : 100BASE-TX full duplex mode, 100BASE-TX
    half duplex mode
Operational MAU type      :
PoE support                : NO
Link aggregation supported : YES
Link aggregation enabled  : NO
Aggregation port ID       : 0
Maximum frame Size        : 1500
```

```

LLDP-MED organizationally information
Power-via-MDI device type   : PD
Power-via-MDI power source  : Local
Power-via-MDI power priority :
Power-via-MDI power value   :
Model name                  : Model name

```

**show lldp local-information** command output description:

Field	Description
Chassis ID type	Chassis ID type for identifying the Chassis ID field
Chassis ID	Used to identify the device, and is generally represented with MAC address
System name	Name of the sending device
System description	Description of the sending device, including hardware/software version, operating system and etc.
System capabilities supported	Capabilities supported by the system
System capabilities enabled	Capabilities currently enabled by the system
LLDP-MED capabilities	LLDP-MED capabilities supported by the system
Device class	MED device class, which is divided into 2 categories: network connectivity device and terminal device. Network connectivity device <ul style="list-style-type: none"> <li>● Class I: normal terminal device</li> <li>● Class II: media terminal device; besides Class I capabilities, it also supports media streams.</li> <li>● Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication.</li> </ul>
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Device manufacturer
Asset tracking identifier	Asset tracking ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Management address subtype	Management address type
Management address	Management address
Interface numbering subtype	Type of the interface identified by the management address
Interface number	ID of the interface identified by the management address
Object identifier	ID of the object identified by the management address

Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID	Port and Protocol VLAN ID
PPVID Supported	Indicates whether port and protocol VLAN is supported <ul style="list-style-type: none"> <li>● Yes: Supported .</li> <li>● No: Not supported.</li> </ul>
PPVID Enabled	Indicates whether port and protocol VLAN is enabled <ul style="list-style-type: none"> <li>● Yes:Enabled.</li> <li>● No: Disabled.</li> </ul>
VLAN name of VLAN 1	Name of VLAN 1
Protocol Identity	Protocol identifier
Auto-negotiation supported	Indicates whether auto-negotiation is supported <ul style="list-style-type: none"> <li>● Yes: Supported.</li> <li>● No: Not supported.</li> </ul>
Auto-negotiation enabled	Indicates whether auto-negotiation is enabled <ul style="list-style-type: none"> <li>● Yes:Enabled.</li> <li>● No: Disabled.</li> </ul>
PMD auto-negotiation advertised	Auto-negotiation advertising capability of the port
Operational MAU type	Speed and duplex state of the port
PoE support	Indicates whether POE is supported <ul style="list-style-type: none"> <li>● Yes: Supported.</li> <li>● No: Not supported.</li> </ul>
Link aggregation supported	Indicates whether link aggregation is supported <ul style="list-style-type: none"> <li>● Yes:Supported.</li> <li>● No: Not supported.</li> </ul>
Link aggregation enabled	Indicates whether link aggregation is enabled <ul style="list-style-type: none"> <li>● Yes: Enabled.</li> <li>● No: Disabled.</li> </ul>
Aggregation port ID	ID of the link aggregation port
Maximum frame Size	Maximum frame size supported by the port
Power-via-MDI device type	Device type, including: PSE (power sourcing equipment) PD (powered device)
Power-via-MDI power source	Power source type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Available power on port
Model name	Name of model

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A



## 1.26 show lldp location

Use this command to display the common LLDP address or emergency number of the local device.

```
show lldp location { civic-location | elin } { identifier id | interface interface-type interface-number
| static }
```

Parameter	Parameter	Description
Description	<b>civic-location</b>	Encapsulates a common address of a network device.
	<b>elin</b>	Encapsulates an emergency number.
	<b>identifier</b> <i>id</i>	Displays one address or emergency number configured. Policy ID of configured information
	<b>interface</b> <i>interface-type interface-number</i>	Displays the address or emergency number on an interface.
	<b>static</b>	Displays all addresses or emergency numbers configured.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** If the policy ID is specified, the specified address or emergency number is displayed.  
 If the interface name is specified, the address or emergency number configured on the interface is displayed.  
 If no parameter is specified, all addresses or emergency numbers are displayed.

**Configuration** The following example displays all addresses.

### Examples

```
Hostname# show lldp location civic-location static
LLDP Civic location information
-----
Identifier      : testt
County         : china
City Division   : 22
Leading street direction : 44
Street number   : 68
Landmark        : 233
Name           : liuy
Building        : 19bui
Floor           : 1
Room            : 33
City            : fuzhou
Country         : 86
Additional location : aaa
Ports           : Gi0/1
-----
```

```
Identifier      : tee
-----
```

The following example displays all emergency numbers.

```
Hostname# show lldp location elin static
Elin location information
-----
Identifier : t
Elin      : iiiiivviii
Ports     : Gi1/0/3
-----
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.27 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

**show lldp neighbors** [ **interface** *interface-type interface-number* ] [ **detail** ]

Parameter	Parameter	Description
<b>Description</b>	<b>interface</b> <i>interface-type interface-number</i>	Interface name
	<b>detail</b>	All detailed information about a neighboring device

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** If the **detail** parameter is not specified, the brief information about a neighboring device is displayed. If the **detail** parameter is specified, the detailed information about a neighboring device is displayed. If the **interface** *interface-type interface-number* parameter is specified, the neighboring device information received on the specified interface is displayed.

**Configuration Examples** The following example displays the neighboring device information received on all ports.

```
Hostname# show lldp neighbors detail
Lldp neighbor-information of port [GigabitEthernet 0/1]
Neighbor index      : 1
Device type         : LLDP Device
```

```
Update time      : 1hour 53minutes 30seconds
Aging time      : 5seconds

Chassis ID type  : MAC address
Chassis id      : 00d0.f822.33cd
System name     : System name
System description : System description
System capabilities supported : Repeater, Bridge, Router
System capabilities enabled : Repeater, Bridge, Router

Management address subtype : 802 mac address
Management address  : 00d0.f822.33cd
Interface numbering subtype :
Interface number    : 0
Object identifier   :

LLDP-MED capabilities :
Device class       :
HardwareRev       :
FirmwareRev       :
SoftwareRev       :
SerialNum         :
Manufacturer name  :
Asset tracking identifier :

Port ID type      : Interface name
Port id          : GigabitEthernet 0/1
Port description  :

802.1 organizationally information
Port VLAN ID     : 1
Port and protocol VLAN ID (PPVID) : 1
  PPVID Supported : YES
  PPVID Enabled   : NO
VLAN name of VLAN 1 : VLAN0001
Protocol Identity :

802.3 organizationally information
Auto-negotiation supported : YES
Auto-negotiation enabled   : YES
PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX
  full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex
  mode, 10BASE-T half duplex mode
Operational MAU type : speed(1000)/duplex(Full)
```

```

PoE support      : NO
Link aggregation supported : YES
Link aggregation enabled : NO
Aggregation port ID : 0
Maximum frame Size : 1500
LLDP-MED organizationally information
Power-via-MDI device type :
Power-via-MDI power source :
Power-via-MDI power priority :
Power-via-MDI power value :

```

## Description of fields:

Field	Description
Neighbor index	Neighbor index
Device type	Type of neighboring device
Update time	Latest update time of neighbor information
Aging time	Aging time of a neighbor, namely the time after which a neighbor is aged and deleted
Chassis ID type	Chassis ID type
Chassis ID	Used to identify a device. Usually, a MAC address is used.
System name	Device name
System description	Device description, including hardware/software version and operating system
System capabilities supported	Functions supported by the system
System capabilities enabled	Functions enabled by the system
Management address subtype	Type of management address
Management address	Management address
Interface numbering subtype	Interface type of management address
Interface number	Interface ID of management address
Object identifier	Object ID of management address
Device class	MED device type: network connectivity device and terminal device Network connectivity device: <ul style="list-style-type: none"> <li>● Class I: general terminal device</li> <li>● Class II: media terminal device, including capabilities of Class I and supporting media stream</li> <li>● Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication</li> </ul>
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name

Asset tracking identifier	Asset ID
Port ID type	Port ID type
Port ID	Port ID
Port description	Port description
Port VLAN ID	VLAN ID of a port
Port and protocol VLAN ID	Port and protocol VLAN ID
PPVID Supported	Whether port and protocol VLAN is supported
PPVID Enabled	Whether port and protocol VLAN is enabled
VLAN name of VLAN 1	VLAN 1 name
Protocol Identity	Protocol ID
Auto-negotiation supported	Whether auto-negotiation is supported
Auto-negotiation enabled	Whether auto-negotiation is enabled
PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
Operational MAU type	Rate and duplex status of port auto-negotiation
PoE support	Whether POE is supported
Link aggregation supported	Whether link aggregation is supported
Link aggregation enabled	Whether link aggregation is enabled
Aggregation port ID	ID of link aggregation port
Maximum frame Size	Maximum frame length supported by a port
Power-via-MDI device type	Device type, including: <ul style="list-style-type: none"> <li>● PSE</li> <li>● PD</li> </ul>
Power-via-MDI power source	Power type
Power-via-MDI power priority	Power supply priority
Power-via-MDI power value	Power value of a port where power is supplied

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.28 show lldp network-policy

Use this command to display the information about an LLDP network policy.

**show lldp network-policy** { **profile** [ *profile-num* ] | **interface** *interface-type interface-number* }

Parameter Description	Parameter	Description
	<b>profile</b> [ <i>profile-num</i> ]	The information about the specified network policy is displayed. The network policy ID ranges from 1 to 1024.
	<b>interface</b> <i>interface-type interface-number</i>	Name of interface.

- Defaults** N/A
- Command Mode** All modes except the user EXEC mode
- Usage Guide**
  - If the ID of a network policy is specified, the information about the specified network policy is displayed.
  - If no parameter is specified, the information about all network policies is displayed.

**Configuration** The following example displays the information about a Network Policy.

**Examples**

```

Hostname# show lldp network-policy profile
Network Policy Profile 1
voice vlan 2 cos 4 dscp 6
voice-signaling vlan 2000 cos 4 dscp 6
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.29 show lldp statistics

The following example displays LLDP statistics.

**show lldp statistics [ global | interface *interface-type interface-number* ]**

Parameter Description	Parameter	Description
	<b>global</b>	Displays the global LLDP statistics.
	<b>interface <i>interface-type interface-number</i></b>	Displays the LLDP statistics of the specified interface.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

- Usage Guide**
  - If the **global** parameter is specified, all LLDP statistics are displayed.
  - If the **interface *interface-type interface-number*** parameter is specified, the LLDP statistics of the specified interface is displayed.

**Configuration** The following example displays all LLDP statistics.

**Examples**

```

Hostname# show lldp statistics
    
```

```
lldp statistics global Information:
Neighbor information last changed time : 1hour 52minute 22second
The number of neighbor information inserted : 2
The number of neighbor information deleted : 0
The number of neighbor information dropped : 0
The number of neighbor information age out : 1

-----

Lldp statistics information of port [GigabitEthernet 0/1]
-----

The number of lldp frames transmitted : 26
The number of frames discarded : 0
The number of error frames : 0
The number of lldp frames received : 12
The number of TLVs discarded : 0
The number of TLVs unrecognized : 0
The number of neighbor information aged out : 0
```

**show lldp statistics** command output description:

Field	Description
Neighbor information last change time	Time the neighbor information is latest updated
The number of neighbor information inserted	Number of times of adding neighbor information
The number of neighbor information deleted	Number of times of removing neighbor information
The number of neighbor information dropped	Number of times of dropping neighbor information
The number of neighbor information aged out	Number of the neighbor information entries that have aged out
The number of lldp frames transmitted	Total number of the LLDPDUs transmitted
The number of frames discarded	Total number of the LLDPDUs discarded
The number of error frames	Total number of the LLDP error frames received
The number of lldp frames received	Total number of the LLDPDUs received
The number of TLVs discarded	Total number of the LLDP TLVs dropped
The number of TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized
The number of neighbor information aged out	Number of the neighbor information entries that have aged out

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.30 show lldp status

Use this command to display LLDP status information.

**show lldp status** [ **interface** *interface-type interface-number* ]

Parameter	Parameter	Description
<b>Description</b>	<b>interface</b> <i>interface-type interface-number</i>	Displays the LLDP status information of the specified interface.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** If the **interface** *interface-type interface-number* parameter is specified, the LLDP status information of the specified interface is displayed.  
 If the **interface** is not specified, the LLDP statuses of all interfaces are displayed.

**Configuration Examples** The following example displays LLDP status information of all ports.

### Examples

```

Hostname# show lldp status
Global status of LLDP      : Enable
Neighbor information last changed time : 1hour 52minute 22second
Transmit interval         : 30s
Hold multiplier           : 4
Reinit delay              : 2s
Transmit delay            : 2s
Notification interval     : 5s
Fast start counts         : 3
-----
Port [GigabitEthernet 0/1]
-----
Port status of LLDP      : Enable
Port state               : UP
Port encapsulation       : Ethernet II
Operational mode         : RxAndTx
Notification enable      : NO
Error detect enable      : YES
Number of neighbors      : 1
Number of MED neighbors  : 0
  
```



**show lldp status** command output description:

Field	Description
Global status of LLDP	Whether LLDP is globally enabled
Neighbor information last changed time	Time the neighbor information is latest updated
Transmit interval	LLDPDU transmit interval
Hold multiplier	TTL multiplier
Reinit delay	Port re-initialization delay
Transmit delay	LLDPDU transmit delay
Notification interval	Interval for sending LLDP trap transmission.
Fast start counts	The number of fast sent LLDPDUs
Port status of LLDP	Whether LLDP is enabled on the port
Port state	Link status of port: UP or DOWN
Port encapsulation	LLDPDU encapsulation format
Operational mode	Operating mode of LLDP
Notification enable	Whether LLDP trap function is enabled on the port
Error detect enable	Whether error detection is enabled on the port
Number of neighbors	Number of neighbors
Number of MED neighbors	Number of MED neighbors

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.31 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

**show lldp tlv-config** [ **interface** *interface-type interface-number* ]

Parameter Description	Parameter	Description
	<b>interface</b> <i>interface-type interface-number</i>	Displays the LLDP TLV configuration of the specified interface.

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** If the **interface** *interface-type interface-number* parameter is specified, the LLDP TLV configuration of the specified interface is displayed.  
If the **interface** parameter is not specified, the LLDP TLV configuration of all interfaces is displayed.

**Configuration** The following example displays TLV information of port 1.

**Examples**

```

Hostname# show lldp tlv-config interface GigabitEthernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
-----
      NAME      STATUS DEFAULT
-----
Basic optional TLV:
Port Description TLV          YES YES
System Name TLV              YES YES
System Description TLV       YES YES
System Capabilities TLV      YES YES
Management Address TLV      YES YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV             YES YES
Port And Protocol VLAN ID TLV YES YES
VLAN Name TLV                YES YES

IEEE 802.3 extend TLV:
MAC-Physic TLV               YES YES
Power via MDI TLV            YES YES
Link Aggregation TLV         YES YES
Maximum Frame Size TLV       YES YES

LLDP-MED extend TLV:
Capabilities TLV              YES YES
Network Policy TLV           YES YES
Location Identification TLV   NO NO
Extended Power via MDI TLV    YES YES
Inventory TLV                 YES YES
    
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

### 1.32 voice vlan

Use this command to configure the LLDP Network Policy. Run the **no** form of this command to remove this configuration.

**{ voice | voice-signaling } vlan { { { vlan-id | dot1p } [ cos cos | dscp dscp ] } | untagged | none }**

**no { voice | voice-signaling } vlan**

Parameter	Parameter	Description
Description	<b>voice</b>	Applies a policy to a voice VLAN.
	<b>voice-signaling</b>	Specifies the voice-signaling application type.
	<i>vlan-id</i>	ID of the VLAN where the voice stream is transmitted. The value range is from 1 to 4094. This VLAN ID will be added to voice packets.
	<b>dot1p</b>	Sets the VLAN ID in the VLAN tag to 0. This tag frame contains only the following priority information: <i>cos</i> and <i>dscp</i> .
	<b>cos</b> <i>cos</i>	Configures the Class of Service (CoS) value for the voice stream in a voice VLAN. The value range is from 0 to 7, and the default value is 5. A larger value indicates a higher priority. The CoS value is 0 for a common VLAN packet, indicating the lowest priority. By default, the CoS value of the voice stream packets transmitted to a voice VLAN is raised to 6, higher than the priority of a common VLAN packet. The CoS value indicates the L2 priority and is saved in the L2 header of a packet. It is filled in the <b>PRI</b> field of the IEEE 802.1Q VLAN tag.
	<b>dscp</b> <i>dscp</i>	Configures the Differentiated Services Code Point (DSCP) for the voice stream in a voice VLAN. The value range is from 0 to 63, and the default value is 46. A larger value indicates a higher priority. The DSCP value is 0 for a common IP packet, indicating the lowest priority. By default, the DSCP value of the voice stream packets transmitted to a voice VLAN is 46, higher than the priority of a common IP packet. The DSCP value indicates the IP priority (IP PRE) and is saved in the L3 header of a packet. For an IPv4 packet, the DSCP value is filled in the first six bits (bit 0 to bit 5) in the <b>ToS</b> field of the IPv4 packet header. For an IPv6 packet, the DSCP value is filled in the first six bits in the <b>Traffic Class</b> field of the IPv6 packet header.
	<b>untagged</b>	Configures a VoIP device to transmit untagged frames. In this case, the VLAN ID and CoS value are ignored.
	<b>none</b>	Indicates that no network policy is delivered, and the VoIP device determines the frames to be sent according to its configuration.

**Defaults** No voice VLAN policy is configured by default.

**Command Mode** LLDP Network Policy configuration mode

**Usage Guide** Configure an LLDP network policy after entering the LLDP network policy configuration mode.

If a device is connected to an IP phone in the downlink direction and the IP phone supports LLDP-MED, you can configure the Network Policy TLV to deliver a policy to the IP phone so that the IP phone changes the voice stream tag and QoS. The configuration procedure is as follows:

- Enable the voice VLAN function, and add the interface connected to the IP phone to the voice VLAN statically. For configuration details, see "Configuring Voice VLAN" in "Ethernet Switch."

- Configure the interface connected to the IP phone as an QoS trust interface (you are advised to use the DSCP trust mode). For configuration details, see "Configuring QoS" in "ACL and QoS."
- If 802.1x authentication is enabled on this interface, you also need to configure a secure channel to allow packets in the voice VLAN to pass. For details, see "Configuring ACL" in "ACL and QoS".
- If the IP phone does not support LLDP-MED, be sure to enable the voice VLAN function and add the MAC address of the IP phone to the voice VLAN OUI list manually.

**Configuration Examples** The following example configures LLDP network policy 1, in which untagged frames need to be transmitted, the VLAN ID is set to 3, CoS is set to 4, and DSCP is set to 6.

```

Hostname#config
Hostname(config)#lldp network-policy profile 1
Hostname(config-lldp-network-policy)# voice vlan untagged
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Hostname(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6
    
```

**Related**

Command	Description
<b>show lldp network-policy profile</b> [ <i>profile-num</i> ]	Displays the LLDP network policy.

**Commands**

**Platform** N/A

**Description**



# IP Service Commands

---

1. ARP Commands
2. ARP Proxy Commands
3. IPv4 Basics Commands
4. NAT Commands
5. DHCP Commands
6. DHCP Snooping Commands
7. DNS Commands
8. DNS Snooping Commands
9. IPv6 Basics Commands
10. DHCPv6 Commands
11. ND Proxy Commands
12. TCP Commands
13. IP REF Commands
14. FPM Commands

# 1 ARP Commands

## 1.1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the **no** form of this command to restore the default setting.

**arp** *ip-address* *MAC-address* *type*

**no arp** *ip-address*

Parameter	Parameter	Description
Description	<i>ip-address</i>	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
	<i>MAC-address</i>	48-bit data link layer address
	<i>type</i>	ARP encapsulation type. The keyword is arpa for the Ethernet interface.

**Defaults** There is no static mapping record in the ARP cache table by default.

**Command Mode** Global configuration mode.

**Default Level** 2

**Usage Guide** RGOS finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table. Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The **clear arp-cache** command can be used to delete the ARP mapping that is learned dynamically.

**Configuration** The following example sets an ARP static mapping record for a host in the Ethernet.

**Examples**

```
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

**Verification** Run the **show arp** command to check the configuration.

**Prompts** 1. If the ARP entry does not exist or is reserved, the following prompt will be displayed:

```
Cannot remove ARP. ARP entry does not exist or reserved.
```

2. When ARP cache table is full or the IP address is a local address, the ARP entry cannot be added. The following prompt will be displayed:

```
Cannot add static ARP.
```

Related Commands	Command	Description
	clear arp-cache	Clears the ARP cache table

**Platform** N/A

**Description**

## 1.2 arp cache interface-limit

Use this command to set the maximum number of ARP learned on the interface.

Use the **no** form of this command to restore the default setting.

**arp cache interface-limit** *limit*

**no arp cache interface-limit**

Parameter	Parameter	Description
<b>Description</b>	<i>limit</i>	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited.

**Defaults** The default is 0.

**Command Mode** Interface configuration mode

**Default Level** 2

**Usage Guide** This function can prevent ARP attacks from generating ARP entries to consume memory. *limit* must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.

**Configuration Examples** The following example sets the maximum number of ARP learned on the interface to 300.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# arp cache interface-limit 300

```

The following example restores the default setting.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# no arp cache interface-limit

```

**Verification** Run the **show arp** command to check the configuration.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.3 arp gratuitous-send interval

Use this command to set the interval of sending the free ARP request message on the interface. Use the **no** form of this command to restore the default setting.

**arp gratuitous-send interval** *seconds* [ *number* ]

**no arp gratuitous-send**

Parameter	Parameter	Description
Description	<i>seconds</i>	The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds.
	<i>number</i>	The number of free ARP request messages to be sent in the range from 1 to 100 in the unit of seconds. The default value is 1.

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode.

**Default Level** 2

**Usage Guide** If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.

**Configuration Examples** The following example sets to send one free ARP request to BVI 1 per second.

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to BVI 1.

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# no arp gratuitous-send
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.4 arp retry interval

Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the **no** form of this command to restore the default setting.



**arp retry interval** *seconds*

**no arp retry interval**

Parameter	Parameter	Description
Description	<i>seconds</i>	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.

**Defaults** The default is 1.

**Command Mode** Global configuration mode.

**Default Level** 2

**Usage Guide** The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.

**Configuration Examples** The following example sets the retry interval of the ARP request as 30 seconds.

```
Hostname(config)# arp retry interval 30
```

Related Commands	Command	Description
	<b>arp retry times</b>	Number of times for retransmitting an ARP request message.

**Platform Description** N/A

## 1.5 arp retry times

Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the **no** form of this command to restore the default setting.

**arp retry times** *number*

**no arp retry times**

Parameter	Parameter	Description
Description	<i>number</i>	The times of sending the same ARP request in the range from 1 to 100. When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent. The default is 5.

**Defaults** The default is 5.

**Command** Global configuration mode.

**Mode****Default Level** 2

**Usage Guide** The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.

**Configuration** The following example sets the local ARP request not to be retried.

**Examples**

```
Hostname(config)# arp retry times 1
```

The following example sets the local ARP request to be retried for one time.

```
Hostname(config)# arp retry times 2
```

**Related****Commands**

Command	Description
<b>arp retry interval</b>	Interval for retransmitting an ARP request message

**Platform** N/A**Description**

## 1.6 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache.

Use the **no** form of this command to restore the default setting.

**arp timeout** *seconds*

**no arp timeout**

**Parameter****Description**

Parameter	Description
<i>seconds</i>	The timeout is in the range from 0 to 2147483 in the unit of seconds.

**Defaults** The default is 3600.

**Command** Interface configuration mode/Global configuration mode.

**Mode****Default Level** 2

**Usage Guide** The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement.

The ARP aging time can be configured globally and on a specified interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the ARP aging time is set to 3,000 seconds in global configuration mode and to 1,800

seconds on interface 1, the ARP aging time of interface 1 is 1800s. The ARP aging time of other interfaces (including new interfaces) is subject to the global ARP aging time, that is, 3,000s.

**Configuration Examples** The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from BVI 1 to 120 seconds.

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# arp timeout 120
```

The following example sets the ARP aging time to 3,000 seconds globally. If no aging time is configured for an interface, the ARP aging time is 3000 seconds for all Layer 3 interfaces.

```
Hostname(config)# arp timeout 3000
```

**Verification** Run the **show arp timeout** command to display that the timeout is set to 3000 seconds for Interface 1.

Related Commands	Command	Description
	<b>clear arp-cache</b>	Clears the ARP cache list.
	<b>show interface</b>	Displays the interface information.

**Platform Description** N/A

## 1.7 arp trust-monitor enable

Use this command to enable egress gateway trusted ARP. Use the **no** form of this command to restore the default setting.

**arp trust-monitor enable**

**no arp trust-monitor enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Default Level** 2

**Usage Guide** The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.

**Configuration** The following example enables egress gateway trusted ARP.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# arp trust-monitor enable

```

The following example disables ingress gateway trusted ARP.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# no arp trust-monitor enable

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.8 arp unresolve

Use this command to set the maximum number of the unresolved ARP entries. Use **no** form of this command to restore the default setting.

**arp unresolve** *number*

**no arp unresolve**

**Parameter  
Description**

Parameter	Description
<i>number</i>	The maximum number of the unresolved ARP entries in the range from 1 to 1024.

**Defaults**

The default is the ARP table size supported by the device.

**Command  
Mode**


Global configuration mode.

**Default Level**

2

**Usage Guide**

If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.

 If the number of unresolved ARP entries is limited, it will affect the maximum number of neighbor addresses that can be resolved simultaneously by the device. The smaller the upper limit, the fewer neighbor addresses that can be resolved at the same time. If the device needs to resolve a large number of neighbor addresses, any portion of it that exceeds the upper limit will be resolved after the existing neighbor addresses to be successfully resolved or the resolution time expires. As a result, the time required to complete all neighbor address resolution will be longer than the time needed when the limit is not set. Users should configure this function as required.

**Configuration**

The following example sets the maximum number of the unresolved items to 500.

**Examples**

```

Hostname(config)# arp unresolve 500

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.

**clear arp-cache** [ **interface** *interface-name* / [ **trusted** ] *ip* [ *mask* ] ]

Parameter Description	Parameter	Description
	<b>trusted</b>	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
	<i>ip</i>	Deletes ARP entries of the specified IP address. If <i>trusted</i> value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
	<i>mask</i>	Deletes ARP entries in a subnet mask. If <i>trusted</i> value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
	<b>interface</b> <i>interface-name</i>	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** On a NFPP-based (Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two **clear arp** times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.

**Configuration Examples** The following example deletes all dynamic ARP mapping records.

```
Hostname# clear arp-cache
```

The following deletes the dynamic ARP entry 1.1.1.1.

```
Hostname# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SVI1.

```
Hostname# clear arp-cache interface vlan 1
```

Related	Command	Description
Commands	<b>arp</b>	Adds a static mapping record to the ARP cache table.

**Platform** N/A

**Description**

## 1.10 ip proxy-arp

Use this command to enable ARP proxy function on the interface. Use the **no** form of this command to restore the default setting.

**ip proxy-arp**

**no ip proxy-arp**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Default Level** 2

**Usage Guide** Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

**Configuration** The following example enables ARP on BVI 1.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip proxy-arp

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.11 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

**show arp** [ *interface-type interface-number* | **trusted** [ *ip [mask]* ] ] | *mac-address* | **static** | **complete** | **incomplete** ] ]

Parameter	Parameter	Description
Description	<i>interface-type</i> <i>interface-number</i>	Displays the ARP entry of a specified Layer-2 or Layer-3 port.
	<b>trusted</b>	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
	<i>ip</i>	Displays the ARP entry of the specified IP address. If <b>trusted</b> is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	<i>mask</i>	Displays the ARP entries of the network segment included within the mask. If <b>trusted</b> is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	<b>static</b>	Displays all the static ARP entries.
	<b>complete</b>	Displays all the resolved dynamic ARP entries.
	<b>incomplete</b>	Displays all the unresolved dynamic ARP entries.
	<i>mac-address</i>	Displays the ARP entry with the specified mac address.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 1

**Usage Guide** Use this command to display the ARP cache table. The **complete** parameter displays all the resolved dynamic ARP entries. The **incomplete** parameter displays all the unresolved dynamic ARP entries

**Configuration Examples** The following example displays the output result of the **show arp** command:

```

Hostname# show arp
Total Numbers of Arp: 7
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1
Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1

```

The following example displays the output result of **show arp 192.168.195.68**

```

Hostname# show arp 192.168.195.68
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 1 0013.20a5.7a5f arpa VLAN 1

```

The following example displays the output result of **show arp 192.168.195.0 255.255.255.0**

```

Hostname# show arp 192.168.195.0 255.255.255.0
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa VLAN 1
Internet 192.168.195.51 1 0018.8b82.8691 arpa VLAN 1

```

The following example displays the output result of **show arp 001a.a0b5.378d**

```

Hostname# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1

```

The following example displays the output result of **show arp static**

```

Hostname# show arp static
Protocol Address Age(min) Hardware Type Interface Origin
Internet 192.168.23.55 <static> 0000.0000.0010 arpa VLAN 100
Configure
Internet 192.168.23.56 <static> 0000.0000.0020 arpa VLAN 100
Authentication
Internet 192.168.23.57 <static> 0000.0000.0020 arpa VLAN 100
DHCP-Snooping
2 static arp entries exist.

```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses
Interface	Layer 3 interface of the ARP entry. For a static ARP entry, this field may be empty, because the IP address of the static ARP entry is not in any directly connected network segment of the device.
Origin	Origin of ARP entries.

**Related  
Commands**

Command	Description
N/A	N/A



**Platform** N/A  
**Description**

## 1.12 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

### show arp counter

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 1

**Usage Guide** N/A

**Configuration Examples** The following example displays the output result of the **show arp counter** command:

```

Hostname# show arp counter
ARP Limit:                75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total:                    1

```

For products that support VXLAN, the number of ARP entries for VXLAN and non-VXLAN are distinguished. The **overlay** field indicates the number of ARP entries for VXLAN, while the **underlayer** field indicates the number of ARP entries for non-VXLAN.

```

Hostname# show arp counter
ARP Limit:                75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total:                    1 (overlay: 0 underlayer: 1)

```

The meaning of each field in the ARP cache table is described in the following Table.

Parameter	Description
overlay	Indicates the number of VxLAN-related ARP entries.
underlayer	Indicates the number of VxLAN-irrelated ARP entries.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.13 show arp packet statistics

Use this command to display the statistics of ARP packets.

**show arp packet statistics** [ *interface-name* ]

Parameter	Parameter	Description
<b>Description</b>	<i>interface-name</i>	Displays the statistics of ARP packets on the specified interface.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Default Level** 1

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output information of the command.

```

Hostname# show arp packet statistics
Interface Received Received Received Sent Sent
Name Requests Replies Others Requests Replies
-----
VLAN 1 10 20 1 50 10
VLAN 2 5 8 0 10 10
VLAN 3 20 5 0 15 12
VLAN 4 5 8 0 10 10
VLAN 5 20 5 0 15 12
VLAN 6 20 5 0 15 12
VLAN 7 20 5 0 15 12
VLAN 8 5 8 0 10 10
VLAN 9 20 5 0 15 12
VLAN 10 20 5 0 15 12
VLAN 11 20 5 0 15 12
VLAN 12 20 5 0 15 12
    
```

Description of fields:

Field	description
Received Requests	Number of received ARP requests

Received Replies	Number of received ARP response messages
Received Others	Number of other received ARP packets
Sent Requests	Number of sent ARP requests
Sent Replies	Number of sent ARP requests

Related Commands	Command	Description
	N/A.	N/A.

**Platform** N/A

**Description**

## 1.14 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

**show arp timeout**

Parameter Description	Parameter	Description
	N/A.	N/A.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode

**Default Level** 1

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of the **show arp timeout** command:

```

Hostname# show arp timeout
Interface arp timeout(sec)
-----

```

```
VLAN 1 3600
```

The meaning of each field in the ARP cache table is described in Table 1.

Related Commands	Command	Description
	N/A.	N/A.

**Platform** N/A

**Description**

## 1.15 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

**show ip arp**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Default Level** 1

**Usage Guide** N/A.

**Configuration Examples** The following example displays the output of **show ip arp**:

```

Hostname# show ip arp
Protocol Address Age (min) Hardware Type Interface
Internet 192.168.7.233 23 0007.e9d9.0488 ARPA GigabitEthernet 0/1
Internet 192.168.7.112 10 0050.eb08.6617 ARPA GigabitEthernet 0/1
Internet 192.168.7.79 12 00d0.f808.3d5c ARPA GigabitEthernet 0/1
Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA GigabitEthernet 0/1
Internet 192.168.7.215 36 00d0.f80d.1090 ARPA GigabitEthernet 0/1
Internet 192.168.7.127 0 0060.97bd.ebee ARPA GigabitEthernet 0/1
Internet 192.168.7.195 57 0060.97bd.ef2d ARPA GigabitEthernet 0/1
Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA GigabitEthernet 0/1

```

The following example displays the output of **show ip arp vrf vpnv4**:

```

Hostname# show ip arp vrf vpnv4
Protocol Address Age (min) Hardware Type Interface
Internet 11.1.1.1 0 78e3.b5b6.f4dc arpa GigabitEthernet
0/1
Internet 11.1.1.2 -- 1111.2222.1111 arpa GigabitEthernet
0/1
Total number of ARP entries: 2

```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically

	configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A.	N/A.

**Platform  
Description** N/A

# 1 ARP Proxy Commands

## 1.1 clear proxy-arp

Use this command to clear a specified proxy ARP entry or all proxy ARP entries.

**clear proxy-arp** [ *ip-address* *vlan-id* ]

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the IP address of the proxy ARP entry. By default, all proxy ARP entries are cleared.
	<i>vlan-id</i>	VLAN ID. The range is from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** When the MAC address of the gateway is changed, you can clear the proxy ARP entry of the gateway to enable the device to learn the correct proxy ARP entry of the gateway as quickly as possible.

**Configuration Examples** The following example clears all proxy ARP entries.

```
Hostname# clear proxy-arp
```

The following example clears a specified proxy ARP entry.

```
Hostname# clear proxy-arp 1.1.1.1 1
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 proxy-arp enable

Use this command to enable Layer-2 ARP Proxy.

**proxy-arp enable**

Use the **no** form of this command to disable Layer-2 ARP Proxy.

**no proxy-arp enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, Layer-2 ARP Proxy is enabled.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables Layer-2 ARP Proxy.

```
Hostname(config)# no proxy-arp enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.3 proxy-arp learn only-wlan

Use this command to enable learning of only ARP entries over wireless ports and ARP entries of special IP addresses over wired ports.

**proxy-arp learn only-wlan [ except ip-address ]**

Use the **no** form of this command to disable the function.

**no proxy-arp learn only-wlan [ except ip-address ]**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Enables learning of ARP entries of specific IP addresses over wired ports at the same time.

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** This function can be enabled when the following conditions are met:

- 1) The AP interconnects with the gateway. The gateway interconnects with the switch. Configure a super VLAN and many sub-VLANs for STAs on the switch;
- 2) The user quantity is large, and therefore the capacity of ARP entries on the ARP proxy easily gets full. To check the capacity, run the show proxy-arp statistics command.

**Configuration Examples** The following example enables learning of only ARP entries over wireless ports and ARP entries of IP addresses 192.168.21.1 and 192.168.22.1.

```

Hostname(config)# proxy-arp learn only-wlan except 192.168.21.1
Hostname(config)# proxy-arp learn only-wlan except 192.168.22.1
    
```

**Verification** Run the **show run** command to check whether the configurations take effect.

### 1.4 show proxy-arp

Use this command to display all proxy ARP entries.

**show proxy-arp** [ *ip\_address* ]

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the IP address of a proxy ARP entry.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all proxy ARP entries.

```

Hostname# show proxy-arp
total entry:2
ip                vid    mac                interface          type
-----
192.168.195.68    1      0013.20a5.7a5f     Gi0/1              DYNAMIC
192.168.195.69    2      0013.20a5.7a51     Gi0/2              DYNAMIC
    
```

Field	Description
-------	-------------



ip	A 32-bit IPv4 address, with 8 bits in one group in decimal format. Groups are separated by dots.
vid	VLAN ID in the range from 1 to 4094.
mac	Hardware address, a 48-bit MAC address, with 16 bits in one group in hexadecimal format. Groups are separated by dots.
interface	Layer 2 interface of the ARP Proxy entry.
type	Dynamic ARP entry only

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A**Description**

## 1.5 show proxy-arp dynamic

Use this command to display the dynamic proxy ARP entry.

**show proxy-arp dynamic**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A**Command Mode** Privileged EXEC mode**Usage Guide** N/A**Configuration** The following example displays the dynamic proxy ARP entry.**Examples**

```

Hostname# show proxy-arp dynamic
ip                mac                type
-----
192.168.195.68    0013.20a5.7a5f    DYNAMIC
192.168.195.69    0013.20a5.7a51    DYNAMIC
total entry: 2

```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.6 show proxy-arp statistics

Use this command to display statistics about the proxy ARP entry.

**show proxy-arp statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can use this command to display statistics about the proxy ARP entry, such as: total proxy ARP entries, next aging time, dropped packet count.

**Configuration Examples** The following example displays statistics about the proxy ARP entry.

```
Hostname# show proxy-arp statistics
total entry: 100
next aging time: 5 seconds
dropped packets: 0
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

# 1 IPv4 Basics Commands

## 1.1 ip address

Use this command to configure the IP address of an interface. Use the **no** form of this command to restore the default setting.

**ip address** *ip-address network-mask* [ **secondary** ]

**no ip address** [ *ip-address network-mask* [ **secondary** ] ]

Parameter Description	Parameter	Description
	<i>ip-address</i>	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
	<i>network-mask</i>	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.

**Defaults** No IP address is configured for the interface by default.

**Command Mode** Interface configuration mode.

**Usage Guide** The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP).

The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value "1" are the network address. The IP address bits that correspond to value "0" are the host address. For example, the network mask of Class A IP address is "255.0.0.0". You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask.

The RGOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction.

Typically, you can try to use secondary IP addresses in the following situations:

A network hasn't enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured.

Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet.

Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.

**Configuration Examples** The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively .

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip address 10.10.10.1 255.255.255.0

```

Related Commands	Command	Description
	<b>show interface</b>	Displays detailed information of the interface.

**Platform Description** N/A

## 1.2 ip address negotiate

Use this command to configure an IP address for the interface through PPP negotiation. Use the **no** form of this command to restore the setting.

**ip address negotiate**

**no ip address negotiate**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example obtains an IP address for the interface through PPP negotiation.

```

Hostname(config)# interface dialer 1
Hostname(config-if-dialer 1)# ip address negotiate

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.3 ip address-pool local

Use this command to enable the IP address pool function. Use the **no** form of this command to disable this function.

**ip address-pool local**

**no ip address-pool local**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function is enabled by default. PPP users can allocate an IP address to the peer end from the IP address pool configured. If you can use the **no ip address-pool local** command to disable this function and clear all configured IP address pools.

**Configuration Examples** The following example enables the IP address pool function.

```
Hostname(config)# ip address-pool local
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.4 ip broadcast-addresss

Use this command to define a broadcast address for an interface in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip broadcast-addresss** *ip-address*

**no ip broadcast-addresss**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Broadcast address of IP network

**Defaults** The default IP broadcast address is 255.255.255.255.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** At present, the destination address of IP broadcast packet is all "1", represented as 255.255.255.255. The RGOS software can generate broadcast packets with other IP addresses through definition, and can receive both all "1" and the broadcast packets defined by itself.

**Configuration Examples** The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip broadcast-address 0.0.0.0

```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.5 ip icmp error-interval

Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the **no** form of this command to restore the default setting.

`ip icmp error-interval DF milliseconds [ bucket-size ]`

**no ip icmp error-interval DF milliseconds [ bucket-size ]**

Use this command to set the rate to send other ICMP error packets. Use the **no** form of this command to restore the default setting.

`ip icmp error-interval milliseconds [bucket-size]`

**no ip icmp error-interval milliseconds [ bucket-size ]**

**Parameter Description**

Parameter	Description
<i>milliseconds</i>	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
<i>bucket-size</i>	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.

**Defaults** The default rate is 10 packets per 100 millisecond.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets.  
If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on

ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.

It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.

**Configuration Examples** The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second.

```
Hostname(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Hostname(config)# ip icmp error-interval 1000 10
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.6 ip icmp timestamp

Use this command to enable the device to return a Timestamp Reply. Use the **no** form of this command to disable returning of Timestamp Reply.

**ip icmp timestamp**  
**no ip icmp timestamp**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example disables the device to return a Timestamp Reply.

```
Hostname(config)# no ip icmp timestamp
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.7 ip directed-broadcast

Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip directed-broadcast** [ *access-list-number* ]

**no ip directed-broadcast**

Parameter	Parameter	Description
Description	<i>access-list-number</i>	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode.

**Usage Guide** IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast. If the **no ip directed-broadcast** command is configured on an interface, RGOS will discard the directed broadcast packets received from the directly connected network.

**Configuration Examples** The following example enables forwarding of directed broadcast packet on the BVI 1 port of a device.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip directed-broadcast
    
```



Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.8 ip local pool

Use this command to create an IP address pool. Use the **no** form of this command to remove the setting.

**ip local pool** *pool-name* *low-ip-address* [ *high-ip-address* ]

**no ip local pool** *pool-name* [ *low-ip-address* [ *high-ip-address* ] ]

Parameter	Parameter	Description
<b>Description</b>	<i>pool-name</i>	Specifies the address pool name. The default name is <b>default</b> .
	<i>low-ip-address</i>	The start IP address in the address pool.
	<i>high-ip-address</i>	(Optional) The end IP address in the address pool.

**Defaults** No IP address pool is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to create one or multiple IP address pools for PPP to allocate addresses to users.

**Configuration Examples** The following example creates an IP address pool named quark ranging from 172.16.23.0 to 172.16.23.255.

```
Hostname(config)#ip local pool quark 172.16.23.0 172.16.23.255
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.9 ip mask-reply

Use this command to configure the RGOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the **no** form of this command to restore the default setting.

**ip mask-reply**

**no ip mask-reply**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Interface configuration mode.	
Usage Guide	Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.	
Configuration Examples	The following example sets the BVI 1 interface of a device to respond the ICMP mask request message.	
	<pre> Hostname(config)# interface bvi 1 Hostname(config-if-BVI 1)# ip mask-reply </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

## 1.10 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the **no** form of this command is restore the default setting.

**ip mtu** *bytes*

**no ip mtu**

Parameter	Parameter	Description
Description	<i>bytes</i>	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes

Defaults	It is the same as the value configured in the interface command <b>mtu</b> by default.	
Command Mode	Interface configuration mode.	
Usage Guide	<p>If an IP packet is larger than the IP MTU, the RGOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface.</p> <p>If the interface configuration command <b>mtu</b> is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if</p>	

the IP MTU value is changed, the MTU value of the interface will remain unchanged.

**Configuration**

The following iexample sets the IP MTU value of the BVI 1 interface to 512 bytes.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip mtu 512
```

**Related  
Commands**

Command	Description
mtu	Sets the MTU value of an interface.

**Platform**

N/A

**Description**

## 1.11 ip redirects

Use this command to allow the RGOS software to send an ICMP redirection message in the interface configuration mode. Use the **no** form of this command to disable this function.

**ip redirects**

**no ip redirects**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

This function is enabled by default.

**Command  
Mode**

Interface configuration mode.

**Usage Guide**

When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.

**Configuration**

The following example disables ICMP redirection for the BVI 1 interface.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# no ip redirects
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.12 ip redirect-drop

Run the **ip redirect-drop** command to enable the routed port protection function.

**ip redirect-drop**

Run the **no** command to disable this feature.

**no ip redirect-drop**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Interface configuration mode	
<b>Default Level</b>	2	
<b>Usage Guide</b>	Run the <b>ip redirect-drop</b> command to enable the routed port protection function on a device port to avoid packets transmitted and received on the same port..	
<b>Configuration Examples</b>	The following example enables the routed port protection function on port GigabitEthernet 0/1	
	<pre> Hostname(config)# interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ip redirect-drop </pre>	
<b>Related Commands</b>	Run the <b>show running-config</b> command to check the configuration.	
<b>Platform Description</b>	N/A	

## 1.13 ip source-route

Use this command to allow the RGOS software to process an IP packet with source route information in global configuration mode. Use the **no** form of this command to disable this function.

**ip source-route**

**no ip source-route**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** RGOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.

**Configuration** The following example disables the IP source route.

**Examples**

```
Hostname(config)# no ip source-route
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.14 ip ttl

Use this command to set the TTL value of the unicast packet. Use the **no** form of this command to restore the default setting.

**ip ttl** *value*

**no ip ttl**

Parameter Description	Parameter	Description
	<i>value</i>	Sets the TTL value of the unicast packet, in the range from 0 to 255.

**Defaults** The default is 64.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the TTL value of the unicast packet to 100.

**Examples**

```
Hostname(config)# ip ttl 100
```

Related	Command	Description
---------	---------	-------------

<b>Commands</b>	N/A	N/A
-----------------	-----	-----

**Platform** N/A

**Description**

## 1.15 ip ttl-expires enable

This command is used to enable notifications of expired TTL. Use the **no** form of this command to disable this function.

**ip ttl-expires enable**

**no ttl-expires enable**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** By default, notifications are enabled to indicate expired TTL.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables notifications indicating expired TTL.

```
Hostname(config)# no ttl-expires enable
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.16 ip unnumbered

This command is used to configure unnumbered interfaces. After an interface is set to an unnumbered interface, IP can be run on the interface and packets can be sent or received on the interface. Use the **no** form of this command to restore the default setting.

**ip unnumbered** *interface-type interface-number*

**no ip unnumbered**

Parameter	Parameter	Description
Description	<i>interface-type</i>	Type of the associated interface
	<i>interface-number</i>	No. of the associated interface

**Defaults** No unnumbered interface is configured by default.

**Command mode** Interface configuration mode

**Usage Guide** An unnumbered interface indicates that IP is enabled on the interface but no IP address is allocated for the interface. An unnumbered interface must associate with an interface with an IP address. The source IP address of the IP packets generated on an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to the unnumbered interface according to the IP address of the associated interface. Pay attention to the following when using an unnumbered interface:

An Ethernet interface cannot be set to an unnumbered interface.

When SLIP, HDLC, PPP, LAPB, and Frame-relay are encapsulated on a serial port, the port can be set to an unnumbered interface. When a frame relay is encapsulated, only a point-to-point subinterface can be set to an unnumbered interface. In the case of X.25 encapsulation, unnumbered interface is not allowed.

The **ping** command cannot be used to check whether an unnumbered interface is working properly because the interface does not have an IP address. The status of an unnumbered interface can be remotely monitored over SNMP.

The network cannot be enabled using an unnumbered interface.

**Configuration Examples** to the following example configures the local interface as an unnumbered interface and sets the associated interface to BVI 1 (an IP address is configured for the interface).

```

Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)# ip unnumbered bvi 1

```

Related Commands	Command	Description
	<b>show interface</b>	Displays the detailed information about the interface.

**Platform** N/A

**Description**

## 1.17 ip unreachable

Use this command to allow the RGOS software to generate ICMP destination unreachable messages. Use the **no** form of this command to disable this function.

**ip unreachable**

**no ip unreachable**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	N/A	N/A
<b>Defaults</b>	This function is enabled by default.	
<b>Command Mode</b>	Interface configuration mode.	
<b>Usage Guide</b>	<p>RGOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message.</p> <p>RGOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing.</p> <p>This command influences all ICMP destination unreachable messages.</p>	
<b>Configuration Examples</b>	<p>The following example disables sending ICMP destination unreachable message on BVI 1.</p> <pre> Hostname(config)# interface bvi 1 Hostname(config-if-BVI-1)# no ip unreachableles </pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.18 peer default ip address

Use this command to allocate an IP address to the peer end through PPP negotiation. Use the **no** form of this command to restore the default setting.

**peer default ip address** { *ip-address* | **pool** [*pool-name*] }

**no peer default ip address**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<i>ip-address</i>	Allocates an IP address to the peer end.
	<i>pool-name</i>	(Optional) Specifies the address pool name. If not specified, the default address pool is used.
<b>Defaults</b>	No IP address is allocated to the peer end through PPP negotiaon by default.	
<b>Command Mode</b>	Dialer interface configuration mode.	
<b>Usage Guide</b>	If the local end is configured with an IP address while the peer end not, you can enable the local end	



to allocate an IP address to the peer end by configuring the **ip address negotiate** command on the peer end and the **peer default ip address** on the local end.

This command is configured on PPP interface supporting encapsulation PPP or SLIP.

The **peer default ip address pool** command is used to allocate an IP address to the peer end from the address pool, configured by using the **ip local pool** command.

The **peer default ip address ip-address** command is used to specify an IP address for the peer end. This command cannot be configured on virtual template interfaces and asyn interfaces.

**Configuration** The following example enables interface dialer 1 to allocate IP address 10.0.0.1 to the peer end.

**Examples**

```
Hostname(config)# interface dialer 1
Hostname(config-if-dialer 1)# peer default ip address 10.0.0.1
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.19 show ip interface

Use this command to display the IP status information of an interface.

**show ip interface** [ *interface-type interface-number* | **brief** ]

**Parameter  
Description**

Parameter	Description
<i>interface-type</i>	Specifies interface type.
<i>interface-number</i>	Specifies interface number.
<i>brief</i>	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

**Defaults** N/A.

**Command  
Mode** Privileged EXEC mode.

**Usage Guide** When an interface is available, RGOS will create a direct route in the routing table. The interface is available in that the RGOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the RGOS software removes the appropriate direct route from the routing table.

If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as "UP". If only the physical line is available, the interface status will be shown as "UP".

The results shown may vary with the interface type, because some contents are the interface-specific options

**Configuration** The following example displays the output of the **show ip interface brief** command.

**Examples**

```

Hostname#show ip interface brief
Interface IP-Address(Pri) IP-Address(Sec) Status Protocol
GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
GigabitEthernet 0/11 no address no address down down
VLAN 1 1.1.1.1/24 no address down down

```

Description of fields:

Field	Description
Status	Link status of an interface. The value can be <b>up</b> , <b>down</b> , or <b>administratively down</b> .
Protocol	IPv4 protocol status of an interface.

The following example displays the output of the **show ip interface vlan** command.

```

SwitchA#show ip interface vlan 1
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
  1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is:
  Proxy ARP is: OFF
  ARP packet input number: 0
  Request packet: 0
  Reply packet: 0
  Unknown packet: 0
  TTL invalid packet number: 0
  ICMP packet input number: 0
  Echo request: 0
  Echo reply: 0
  Unreachable: 0
  Source quench: 0
  Routing redirect: 0

```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface

	hardware status and line protocol status are “UP”.
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachable is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fast switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: Request packet: Reply packet: Unknown packet:	Show the total number of ARP packets received on the interface, including: ARP request packet ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

**Related  
Commands**

Command	Description
N/A.	N/A.

**Platform  
Description**

N/A.

## 1.20 show ip packet queue

Use this command to display the statistics of IP packet queues.

**show ip packet queue**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The following example displays the statistics of IP packet queues.

**Examples**

```

Hostname#show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
Failed to alloc ebuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
    
```

Field	Description
IP packet receive queue	Statistics of received packets
Discards	Statistics of discarded packets
Sent packets	Statistics of sent packets
ICMP error queue	Statistics of ICMP error packets

Related	Command	Description
---------	---------	-------------

<b>Commands</b>	N/A	N/A
-----------------	-----	-----

**Platform** N/A

**Description**

## 1.21 show ip packet statistics

Use this command to display the statistics of IP packets.

**show ip packet statistics** [ **total** | *interface-name* ]

Parameter	Parameter	Description
<b>Description</b>	<i>interface-name</i>	Interface name
	<i>total</i>	Displays the total statistics of all interfaces.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The following example displays the output of this command.

**Examples**

```

Hostname# show ip packet statistics
Total
  Received 1000 packets, 1000000 bytes
  Unicast:1000,Multicast:0,Broadcast:0
  Discards:0
  HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
  NoRoutes:0
  Others:0
  Sent 100 packets, 6000 bytes
  Unicast:50,Multicast:50,Broadcast:0

VLAN 1
  Received 1000 packets, 1000000 bytes
  Unicast:1000,Multicast:0,Broadcast:0
  Discards:0
  HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
  NoRoutes:0
  Others:0
  Sent 100 packets, 6000 bytes
  Unicast:50,Multicast:50,Broadcast:0

```

Related	Command	Description
---------	---------	-------------

<b>Commands</b>	<b>ip default-gateway</b>	Configures the default gateway, which is only supported on the Layer 2 switch.
-----------------	---------------------------	--

**Platform** N/A

**Description**

## 1.22 show ip pool

Use this command to display the IP address pool.

**show ip pool** [ *pool-name* ]

Parameter	Parameter	Description
<b>Description</b>	<i>pool-name</i>	Specifies the IP address pool.

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example displays all IP address ranges.

**Examples**

```

Hostname# show ip pool
Pool          Begin          End              Free   In use
default      1.1.1.1        1.1.1.1         1      0
pool1        2.2.2.2        2.2.2.254      253    0
pool2        3.1.1.1        3.2.1.1        65537  0
pool3        192.168.1.1   192.168.1.254

```

Field	Description
Pool	Address pool name
Begin	The start IP address of the address pool
Free	The number of free IP addresses in the address pool
In use	The number of IP addresses in use in the address pool

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A

**Description**

## 1.23 show ip raw-socket

Use this command to display IPv4 raw sockets.

**show ip raw-socket** [ *num* ]

Parameter	Parameter	Description
Description	<i>num</i>	Protocol.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The following example displays all IPv4 raw sockets.

### Examples

```

Hostname# show ip raw-socket
Number Protocol Process name
1      ICMP    dhcp.elf
2      ICMP    vrrp.elf
3      IGMP    igmp.elf
4      VRRP    vrrp.elf
Total: 4

```

Field Description

Field	Description
Number	Number
Protocol	Protocol
Process name	Process name
Total	Total number

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.24 show ip sockets

Use this command to display all IPv4 sockets.

**show ip sockets**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	N/A.	N/A.
--------------------	------	------

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration** The following displays all IPv4 sockets.

**Examples**

```

Hostname# show ip sockets
Number Process name      Type      Protocol LocalIP:Port  ForeignIP:Port
State
1      dhcp.elf              RAW       ICMP       0.0.0.0:1     0.0.0.0:0
*
2      vrrp.elf              RAW       ICMP       0.0.0.0:1     0.0.0.0:0
*
3      igmp.elf              RAW       IGMP       0.0.0.0:2     0.0.0.0:0
*
4      vrrp.elf              RAW       VRRP       0.0.0.0:112   0.0.0.0:0
*
5      dhcpc.elf            DGRAM    UDP        0.0.0.0:68    0.0.0.0:0
*
6      rg-snmpd             DGRAM    UDP        0.0.0.0:161   0.0.0.0:0
*
7      wbav2                DGRAM    UDP        0.0.0.0:2000  0.0.0.0:0
*
8      vrrp_plus.elf        DGRAM    UDP        0.0.0.0:3333  0.0.0.0:0
*
9      mpls.elf             DGRAM    UDP        0.0.0.0:3503  0.0.0.0:0
*
10     rds_other_th         DGRAM    UDP        0.0.0.0:3799  0.0.0.0:0
*
11     rg-snmpd             DGRAM    UDP        0.0.0.0:14800 0.0.0.0:0
*
12     rg-sshd              STREAM   TCP        0.0.0.0:22    0.0.0.0:0
LISTEN
13     rg-telnetd           STREAM   TCP        0.0.0.0:23    0.0.0.0:0
LISTEN
14     wbard                STREAM   TCP        0.0.0.0:4389  0.0.0.0:0
LISTEN
15     wbard                STREAM   TCP        0.0.0.0:7165  0.0.0.0:0
LISTEN
Total: 15
    
```

Field Description



Field	Description
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.25 show ip udp

Use this command to display IPv4 UDP sockets.

**show ip udp [ local-port num ]**

Use this command to display IPv4 UDP socket statistics.

**show ip udp statistics**

**Parameter  
Description**

Parameter	Description
<b>local-port num</b>	Local port number

**Defaults**

N/A.

**Command Mode**

Privileged EXEC mode.

**Usage Guide**

N/A.

**Configuration**

The following example displays all IPv4 UDP sockets.

**Examples**

```

Hostname# show ip udp
Number Local Address      Peer Address      Process name
1      0.0.0.0:68             0.0.0.0:0        dhcpc.elf
2      0.0.0.0:161           0.0.0.0:0        rg-snmpd
3      0.0.0.0:2000          0.0.0.0:0        wbav2

```

4	0.0.0.0:3333	0.0.0.0:0	vrrp_plus.elf
5	0.0.0.0:3503	0.0.0.0:0	mpls.elf
6	0.0.0.0:3799	0.0.0.0:0	rds_other_th
7	0.0.0.0:14800	0.0.0.0:0	rg-snmpd

## Field Description

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

# 1 NAT Commands

## 1.1 address

Use this command to configure the address range of an empty NAT address pool.

Use the **no** form of this command to delete the address range of an address pool.

**address** *start-ip end-ip* [ **match interface** *interface-type interface-number* ]

**no address** *start-ip end-ip* [ **match interface** *interface-type interface-number* ]

**address interface** *interface* [ **match interface** *interface-type interface-number* ]

**no address interface** *interface* [ **match interface** *interface-type interface-number* ]

**Parameter Description**

Parameter	Description
<i>start-ip</i>	Start IP address of an address block
<i>end-ip</i>	End IP address of an address block
<b>interface</b> <i>interface</i>	Sets the interface used when NAT has multiple outside interfaces. The addresses defined in a pool use interface addresses and are used when the interface addresses are unknown and will be negotiated.  Note that this parameter must be used with the <b>match interface</b> <i>interface</i> parameter, and the two interfaces must be consistent. Otherwise, NAT may fail.
<b>match interface</b> <i>interface</i>	Sets the interface used when NAT has multiple outside interfaces. When the router determines the egress of packets, NAT uses this egress to select an address that matches it from the pool.

**Defaults** No address range is defined by default.

**Command Mode** NAT address pool configuration mode

**Usage Guide** If you need to define multiple address ranges for an address pool, first enter NAT address pool configuration mode, and then define the NAT address ranges. These commands are not supported on aggregate ports.

**Configuration Examples** The following example creates a mulnets address pool and defines two address blocks.

```

Hostname(config)# ip nat pool mulnets netmask 255.255.255.0
Hostname(config-ipnat-pool)# address 172.16.10.1 172.16.10.254
Hostname(config-ipnat-pool)# address 192.168.100.1 192.168.100.50
    
```

Related	Command	Description
---------	---------	-------------

<b>Commands</b>	<b>ip nat pool</b>	Defines the IP NAT address pool.
-----------------	--------------------	----------------------------------

**Platform**  
**Description**

N/A

## 1.2 ip nat

Use this command to perform NAT on an interface.

Use the **no** form of this command to disable NAT on an interface.

**ip nat { inside | outside }**

**no ip nat { inside | outside }**

Parameter	Parameter	Description
<b>Description</b>	<b>inside</b>	Performs NAT on incoming packets.
	<b>outside</b>	Performs NAT on outgoing packets.

**Defaults** NAT is not enabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** The inside and outside interfaces can be configured only for a routing interface. NAT is performed only when packets are routed between outside and inside interfaces and meet a certain rule. Therefore, at least an inside interface and an outside interface must be configured.

**Configuration Examples** The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

The following example (on the switch with a firewall card or wireless device) dynamically translates internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```

Hostname#configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.12.6
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip nat inside
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip address 200.168.12.17
255.255.255.0
Hostname(config-if-GigabitEthernet 0/2)# ip nat outside
Hostname(config-if-GigabitEthernet 0/2)# exit
Hostname(config)# ip nat pool net200 200.168.12.1 200.168.12.15 netmask
255.255.255.0
Hostname(config)# ip nat inside source list 1 pool net200
Hostname(config)# access-list 1 permit 192.168.12.0 0.0.0.255

```

#### Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears the NAT entry table.
<b>ip nat inside destination</b>	Enables NAT for the internal destination address.
<b>ip nat inside source</b>	Enables NAT for internal source addresses.
<b>ip nat outside source</b>	Enables NAT for external source addresses.
<b>ip nat pool</b>	Defines the IP NAT address pool.
<b>show ip nat translations</b>	Displays IP NAT entries.

**Platform** For a router or gateway device, run the **ip nat inside/outside** command on an interface directly. For a firewall card or wireless device, run the **no encapsulation** command on the interface first.

## 1.3 ip nat application

Use this command to implement special application of NAT.

Use the **no** form of this command to cancel this special application.

**ip nat application source list** *list-num* **destination** *global-ip*

{ **dest-change** *ip-address* | **src-change** *ip-address* }

**ip nat application source list** *list-num* **destination** { **tcp** *global-ip port-num* | **udp**

*global-ip port-num* } { **dest-change** *ip-address port-num* | **src-change**

*ip-address* }

**no ip nat application source list** *list-num* **destination** *global-ip*

{ **dest-change** *ip-address* | **src-change** *ip-address* }

**no ip nat application source list** *list-num* **destination** { **tcp** *global-ip port-num* | **udp**

*global-ip port-num* } { **dest-change** *ip-address port-num* | **src-change**

*ip-address* }

Parameter Description	Parameter	Description
	<i>list-num</i>	Access list of internal local addresses, that is, match criteria of the source addresses of packets. The value range is from 1 to 199 and 1300 to 2699.
	<i>global-ip</i>	Internal global address match, that is, match criteria of the destination addresses of packets. NAT entries are created only when the destination IP address matches this address and the source IP address matches the previously defined access list.
	<b>tcp</b> <i>global-ip port-num</i>	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the TCP packet match the criteria defined here and the source address matches the previously defined access list.
	<b>udp</b> <i>global-ip port-num</i>	Matches the internal global address and the destination port. NAT entries are created only when the destination address and port of the UDP packet match the criteria defined here and the source address matches the previously defined access list.
	<b>dest-change</b> <i>ip-address port-num</i>	Changes the destination address and port of the packet that meets criteria.
	<b>src-change</b> <i>ip-address</i>	Changes the source address of the packet that meets criteria.

**Defaults** This rule is not defined by default.

**Command**

**Mode** Global configuration mode

**Usage Guide** In some advanced applications of NAT, it is necessary to change the source or destination addresses of some particular IP packets. This command can be used to perform this operation. The following example uses this command to implement the domain name resolution relay service (DNS relay).

**Configuration Examples** The following example allows the host in the network segment 192.168.1.0 in the internal network to point the DNS server to the IP address 192.168.1.1 of the NAT inside interface. The NAT function of the router forwards the DNS request from the host in the internal network to the true DNS server 202.101.98.55, and forwards the DNS response packet to the host in the internal network. Implement this function with the **ip nat application** command. The semantics is: If there is a UDP packet whose source address meets the criteria of access-list 1, destination address is 192.168.1.1, and destination port is 53, and then change the destination address of this IP packet to

202.101.98.55 and the destination port to 53.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip nat inside
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip address 200.168.12.1
255.255.255.0
Hostname(config-if-GigabitEthernet 0/2)# ip nat outside
Hostname(config-if-GigabitEthernet 0/2)# exit
Hostname(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask
255.255.255.0
Hostname(config)# ip nat inside source list 1 pool net200
Hostname(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Hostname(config)# ip nat application source list 1 destination udp 192.168.1.1
53 dest-change 202.101.98.55 53
Hostname(config)# access-list 1 permit 192.168.1.0 0.0.0.255

```

#### Related Commands

Command	Description
<b>address</b>	Defines the address block range of an address pool.
<b>clear ip nat translation</b>	Clears the NAT entry table.
<b>ip nat</b>	Specifies that NAT should be performed on the traffic that passes this interface.
<b>ip nat inside destination</b>	Enables NAT for the internal destination address.
<b>ip nat inside source</b>	Enables NAT for internal source addresses.
<b>ip nat outside source</b>	Enables NAT for external source addresses.
<b>show ip nat translations</b>	Displays IP NAT entries.

#### Platform

Description N/A

## 1.4 ip nat inside destination

Use this command to enable NAT for the internal destination address.

Use the **no** form of this command to disable NAT for the internal destination address.

**ip nat inside destination list** *access-list-number* **pool** *pool-name*

**no ip nat inside destination list** *access-list-number*

#### Parameter Description

Parameter	Description
<b>list</b> <i>access-list-number</i>	Internal global addresses are defined in the access list. If

	the external network accesses the address in the access list, the internal global address will be translated into the internal local address defined in the pool. Note that here you should use the extended ACL in the range from 100 to 199 whose destination IP address is a virtual IP address.
<b>pool</b> <i>pool-name</i>	A space in the address pool that defines the internal local address. An internal local address will be assigned from this space during destination address translation.

**Defaults** NAT for the internal source address is disabled by default.

**Command**

**Mode** Global configuration mode

**Usage Guide** Translation of internal destination addresses can be performed to realize load balance of TCP traffic. When a host in the internal network is overloaded with TCP traffic, multiple hosts may be required to balance the load of TCP traffic. In this case, you can use NAT to realize load balance of TCP traffic. NAT will create a virtual host to provide the TCP service. This virtual host corresponds to multiple real internal hosts. Then, NAT polls and replaces the destination address, so as to distribute the load. However, no change is made to other IP traffic, unless NAT is configured otherwise. When NAT is configured to realize TCP load balance, the address of the internal network can be either a valid global address or a private network address. However, the address of the virtual host must be a valid global address.

**Configuration Examples** The following example configures the internal network to provide a virtual host address 10.10.10.100 externally. The external network uses this address to access the WWW service. The hosts that provide services in the internal LAN are actually two hosts with the addresses 10.10.10.1 and 10.10.10.2. During NAT, load balance is realized in polling mode.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.10.10.254
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip nat inside
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip address 200.168.12.17
255.255.255.0
Hostname(config-if-GigabitEthernet 0/2)# ip nat outside
Hostname(config-if-GigabitEthernet 0/2)# exit
Hostname(config)# ip nat pool net10 10.10.10.1 10.10.10.2 prefix-length 24
type rotary
Hostname(config)# ip nat inside destination list 100 pool net10
Hostname(config)# access-list 100 permit ip any host 10.10.10.100

```



Related Commands	Command	Description
	<b>clear ip nat translation</b>	Clears the NAT entry table.
	<b>ip nat</b>	Specifies that NAT should be performed on the traffic that passes this interface.
	<b>ip nat inside source</b>	Enables NAT for internal source addresses.
	<b>ip nat outside source</b>	Enable NAT for external source addresses.
	<b>ip nat pool</b>	Defines the IP NAT address pool
	<b>show ip nat translations</b>	Displays IP NAT entries.

### Platform

Description N/A

## 1.5 ip nat inside source

Use this command to enable NAT for internal source addresses in interface configuration mode.

Use the **no** form of this command to disable static or dynamic NAT.

**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [ **overload** ]

**ip nat inside source static** *local-ip global-ip* [ **permit-inside** ] [ **netmask** *mask* | **match** *interface-type interface-number* ]

**ip nat inside source static** *local-ip* **interface** *interface-type interface-number* [ **permit-inside** ]

**ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port* [ **permit-inside** ] [ **match** *interface-type interface-number* | **netmask** *mask* ]

**ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port* [ **permit-inside** ]

**no ip nat inside source list** *access-list-number* [ **interface** *interface-type interface-number* | **pool** *pool-name* ] [ **overload** ]

**no ip nat inside source static** *local-ip global-ip* [ **permit-inside** ] [ **netmask** *mask* | **match** *interface-type interface-number* ]

**no ip nat inside source static** *local-ip* **interface** *interface-type interface-number* [ **permit-inside** ]

**no ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port* [ **permit-inside** ] [ **match** *interface-type interface-number* | **netmask** *mask* ]

**no ip nat inside source static** { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port* [ **permit-inside** ]

### Parameter Description

Parameter	Description
<b>list</b> <i>access-list-number</i>	Specifies the access list of local addresses. NAT entries will be created only for the traffic with the source address that matches this access list. The value range is from 1 to 199 and 1300 to 2699.

<b>interface</b> <i>interface-type interface-number</i>	Uses the global address of the outside interface to perform Network Address Port Translation (NAPT), also called extended NAT.
<b>pool</b> <i>pool-name</i>	Uses a global address in the address pool to perform NAT.
<b>overload</b>	(Optional) Every global address in the pool can be reused for translation, namely, NAPT. Currently, this parameter is not set, and global addresses are reusable. This parameter is added in order to be compatible with the command of Cisco.
<b>static</b> <i>local-ip global-ip</i>	Defines the simple static NAT. <i>local-ip</i> is a local address, and <i>global-ip</i> is a global address. The <b>no</b> form of this command does not check the validity of <i>global-ip</i> .
<b>static</b> <i>protocol</i>	Defines the extended static NAT. <i>protocol</i> can be either TCP or UDP.
<i>local-port</i>	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port.
<i>global-port</i>	Service port number of the global address. The external network accesses the services of hosts in the internal network through this port. This port number can be different from <i>local-port</i> .
<b>permit-inside</b>	Allows users in the internal network to access the host with the IP address indicated by <i>local-ip</i> through <i>global-ip</i> . This keyword appears only in the <b>ip nat inside source static</b> command and is applicable only on routers.
<b>match</b> <i>interface-type interface-number</i>	Specifies the outside interface (used in smart DNS).
<b>netmask</b> <i>mask</i>	Network mask

**Defaults** NAT for internal source addresses is disabled by default.

**Command**

**Mode** Global configuration mode

**Usage Guide** When the IP address of the internal network is a private address and the internal network needs to communicate with the external network, NAT must be configured to translate the internal private IP address into the globally unique IP address.

If organizations, such as net bars or enterprises, access the network only for obtaining resources in the external network, such as browsing Web pages, receiving and sending emails, and downloading files, but not for providing network services for the external network, the IP address of the outside interface can be used directly as the global address and the address is translated in NAPT mode. If

NAT is not configured, the internal network with the private address, even if physically interconnected with the external network, is unable to interwork with the external network, because the external network does not provide network routing for the private address.

Static NAT or NAT should be configured for the internal hosts that provide services. To ensure continuous service provisioning, do not use the address of the outside interface to perform NAT because this address is interconnected with ISP and is very likely to be translated. Generally, users in the internal network can access the services provided by these internal hosts simply by using the IP address of the internal network. However, some special application services can only be accessed by users in the internal network using the global IP address. In this case, you need to add the keyword **permit-inside** when configuring static NAT or static NAT for internal source addresses. Moreover, it is advisable to run the **no ip redirects** command on the inside interface to prevent the inside interface from sending redirection packets.

When multiple consecutive inside network hosts or ports need to provide services to outside networks, you can configure consecutive IP address or port mappings.

**Configuration Examples** The following example dynamically translates the internal host 192.168.12.0/24 to the network segment with the global address 200.168.12.0/28. NAT is not allowed for the hosts in other network segments of the internal network.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.12.6
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip nat inside
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip address 200.168.12.17
255.255.255.0
Hostname(config-if-GigabitEthernet 0/2)# ip nat outside
Hostname(config-if-GigabitEthernet 0/2)# exit
Hostname(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length
28
Hostname(config)# ip nat inside source list 1 pool net200
Hostname(config)# access-list 1 permit 192.168.12.0 0.0.0.255

```

**Related  
Commands**

Command	Description
<b>clear ip nat translation</b>	Clears the NAT entry table.
<b>ip nat</b>	Specifies that the NAT should be performed on the traffic that passes this interface.
<b>ip nat inside destination</b>	Enables NAT for the inside destination address.
<b>ip nat outside source</b>	Enable NAT for external source addresses.
<b>ip nat pool</b>	Defines the IP NAT address pool.
<b>show ip nat translations</b>	Displays IP NAT entries.

**Platform****Description** N/A

## 1.6 ip nat outside source

Use this command to enable NAT for the external source addresses.

Use the **no** form of this command is used to disable NAT for external source addresses.

**ip nat outside source list** *access-list-number* **pool** *pool-name*

**no ip nat outside source list** *access-list-number* [**pool** *pool-name* ]

**ip nat outside source static** *global-ip local-ip*

**no ip nat outside source static** *global-ip local-ip*

**ip nat outside source static** *protocol global-ip global-port local-ip local-port*

**no ip nat outside source static** *protocol global-ip global-port local-ip local-port*

**Parameter  
Description**

Parameter	Description
<b>list</b> <i>access-list-number</i>	Global address access list. NAT entries will be created only for the traffic with the source address that matches this access list. The value range is from 1 to 199 and 1300 to 2699.
<b>pool</b> <i>pool-name</i>	Uses a local address in the address pool to perform NAT.
<b>static</b> <i>global-ip local-ip</i>	Defines the simple static NAT. <i>local-ip</i> is a local address, and <i>global-ip</i> is a global address.
<b>static</b> <i>protocol</i>	Defines the extended static NAT. <i>protocol</i> can be either TCP or UDP.
<i>local-port</i>	Service port number (TCP or UDP) of the local address. Each service typically corresponds to a service port. This port number can be different from <i>global-port</i> .
<i>global-port</i>	Service port number of the global address

**Defaults** NAT for external source addresses is disabled by default.

**Command**

**Mode** Global configuration mode

**Usage Guide**

NAT for external source addresses is mainly used for the overlapped address space. Two private networks to be interconnected are assigned with the same IP address, or a private network and a public network are assigned with the same global IP address, which is called address overlap. Two network hosts with the overlapped address cannot communicate with each other because they both determine that the remote host is located in the local network. Overlapped address NAT is configured to resolve the problem of communication between networks with the overlapped address. With

overlapped address NAT configured, the external network host address behaves like another network host address in the internal network, and vice versa.

Configuration of overlapped address NAT includes two steps: 1) Configure the internal source address NAT; 2) Configure the external source address NAT. The external source address translation can be configured only when the address of the external network is overlapped with that of the internal network. The external source address translation can be configured as static NAT or dynamic NAT.

Address overlap is inevitable when a non-registered global IP address is assigned to connect to the Internet during internal network construction. Because the internal network generally uses the domain name to access the external network host, routers must support NAT for DNS packets.

**Configuration Examples** In the following example, the address of the internal network 92.168.12.0/24 is overlapped with that of the external network. After translation, the internal host can access the host in the network segment 92.168.12.0/24 in the external network through the network address 192.168.12.0/24.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 192.168.12.55
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)# ip nat inside
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface gigabitethernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# ip address 192.168.10.1
255.255.255.0
Hostname(config-if-GigabitEthernet 0/2)# ip nat outside
Hostname(config-if-GigabitEthernet 0/2)# encapsulation ppp
Hostname(config-if-GigabitEthernet 0/2)# exit
Hostname(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length
28
Hostname(config)# ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length
24
Hostname(config)# ip nat inside source list 1 pool net200
Hostname(config)# ip nat outside source list 1 pool net192
Hostname(config)# access-list 1 permit 92.168.12.0 0.0.0.255
Hostname(config)# ip route 192.168.12.0 255.255.255.0 192.168.100.2

```

**Related  
Commands**

Command	Description
<b>clear ip nat translation</b>	Clears the NAT entry table.
<b>ip nat</b>	Specifies that NAT should be performed for the traffic that passes this interface.
<b>ip nat inside destination</b>	Enables NAT for internal destination address.
<b>ip nat inside source</b>	Enables NAT for internal source address.
<b>ip nat pool</b>	Defines the IP NAT address pool.

<b>show ip nat translations</b>	Displays IP NAT entries.
---------------------------------	--------------------------

**Platform****Description** N/A

## 1.7 ip nat pool

Use this command to define an address pool for NAT.

Use the **no** form of this command to delete the address pool.

**ip nat pool** *pool-name* [ *start-ip end-ip* ] { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ]

**ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ]

**ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [ **type rotary** ] [ **hardware** ]

**no ip nat pool** *pool-name*

Parameter	Parameter	Description
<b>Description</b>	<i>pool-name</i>	Name of the NAT address pool
	<i>start-ip</i>	Start IP address of the NAT address pool
	<i>end-ip</i>	End IP address of the NAT address pool
	<b>netmask</b> <i>netmask</i>	Net mask of an address in the NAT address pool
	<b>prefix-length</b> <i>prefix-length</i>	Specifies the length of the network mask of the addresses in the NAT address pool.
	<b>type rotary</b>	Type of the NAT address pool. <b>rotary</b> means round robin. That is, each address has the same probability of being assigned. The type is <b>rotary</b> no matter whether <b>rotary</b> is set. The <b>rotary</b> parameter is introduced in order to keep compatible with the command of Cisco.

**Defaults** No address pool is defined by default.

**Command**

**Mode** Global configuration mode

**Usage Guide** If multiple address blocks must be defined for an address pool, first create an empty address pool, and define the address range.

**Configuration Examples** The following example creates an address pool named **net192**, with the start address 192.168.12.1, end address 192.168.12.254, and a 24-bit net mask.

```

Hostname# configure terminal
Hostname(config)# ip nat pool net192 192.168.12.1 192.168.12.254
prefix-length 24

```

Related Commands	Command	Description
	<b>address</b>	Defines the address block range of an address pool.
	<b>clear ip nat translation</b>	Clears the NAT entry table.
	<b>ip nat</b>	Specifies that NAT should be performed for the traffic that passes this interface.
	<b>ip nat inside destination</b>	Enables NAT for inside destination addresses.
	<b>ip nat inside source</b>	Enables NAT for internal source addresses.
	<b>ip nat outside source</b>	Enables NAT for external source addresses.
	<b>show ip nat statistics</b>	Displays IP NAT statistics.
	<b>show ip nat translations</b>	Displays IP NAT entries.

**Platform**

Description N/A

## 1.8 ip nat keepalive

Use this command to configure the interval of sending gratuitous ARP (GARP) packets with the local address.

**ip nat keepalive** [ *keepalive\_out* ]

**no ip nat keepalive**

**default ip nat keepalive**

Parameter Description	Parameter	Description
	<i>keepalive_out</i>	Sending interval. The value range is from 1 to 86400.

**Defaults** The interval of sending GARP packets with the local address is not configured by default.

**Command**

**Mode** Global configuration mode

**Usage Guide**

Some addresses in NAT rules should be taken as the local address. Sending GARP packets at intervals avoids address conflicts.

**Configuration Examples**

The following example sets the interval of sending GARP packets with the local address to 10 seconds.

```

Hostname# configure terminal
Hostname(config)# ip nat keepalive 10

```

Related Commands	Command	Description
	N/A	N/A

**Platform**  
**Description** N/A

## 1.9 ip nat translation

Use this command to configure the NAT Application Layer Gateway (ALG).

```
ip nat translation { dns [ ttl ttl_time ] | ftp [ port port_num ] | h323 | pptp | rtsp | sip | tftp [ port port_num ] }
```

```
no ip nat translation { dns | ftp | h323 | pptp | rtsp | sip | tftp }
```

Parameter Description	Parameter	Description
	<i>ttl_time</i>	Defines the UDP TTL for DNS. The default is 0.
	<i>port_num</i>	Defines the port number used for the FTP application. The default value is 21.

**Defaults** NAT ALG supports DNS, File Transfer Protocol (FTP), H.323, Point-to-Point Tunneling Protocol (PPTP), Trivial File Transfer Protocol (TFTP), Real Time Streaming Protocol (RTSP), and Session Initiation Protocol (SIP) by default.

### Command

**Mode** Global configuration mode

**Usage Guide** In NAT application, the IP addresses and ports of data packets are changed. However, the IP addresses and ports of certain special protocols are contained in the valid data of the application layer. To successfully perform NAT for such special protocols, the specific protocol gateway needs to be enabled.

The following example configures DNS TTL to 30 seconds.

```
Hostname# configure terminal
Hostname(config)# ip nat translation dns ttl 30
```

### Configuration

#### Examples

The following example configures Port 25 for FTP.

```
Hostname# configure terminal
Hostname(config)# ip nat translation ftp port 25
```

Related Commands	Command	Description
	N/A	N/A

**Platform**  
**Description** N/A



## 1.10 show ip nat translations

Use this command to display NAT translations.

**show ip nat translations** [ *acl\_num* ] [ **gre** | **icmp** | **tcp** | **udp** ] [ **verbose** ]

Parameter	Parameter	Description
Description	<b>icmp</b>	Displays NAT entries only for ICMP.
	<b>tcp</b>	Displays NAT entries only for TCP.
	<b>udp</b>	Displays NAT entries only for UDP.
	<b>gre</b>	Displays NAT entries only for GRE.
	<i>acl_num</i>	ACL number, which supports only the extended ACL to filter the displayed content. The value range is from 100 to 199.
	<b>verbose</b>	Displays more detailed NAT entries.
	<i>dev_id</i>	Device ID
	<i>slot_id</i>	Slot ID of service card

**Defaults** N/A

### Command

**Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the summary of IP NAT entries, such as protocols, internal global addresses and port numbers, internal local addresses and port numbers, external local addresses and port numbers, and external global addresses and port numbers. Used with the **verbose** parameter, it displays more detailed information, including the timeout period configured for each entry, remaining time for this entry, and flag of the entry.

**Configuration** The following example displays NAT translations.

### Examples

```

Hostname# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global      Inside local      Outside local      Outside global
timeout vrf
tcp 192.168.5.103:1987 192.168.211.21 :1987 211.67.71.7 :80
211.67.71.7:80 timeout=85139 1
udp 192.168.5.103:1041 192.168.211.183:1041 202.101.98.55 :53
202.101.98.55:53 timeout=38 1

```

## Field Description

Field	Description
Pro	Protocol type. <b>udp</b> indicates the UDP translation entry. <b>tcp</b> indicates the TCP translation entry. <b>icmp</b> indicates the ICMP translation entry.
Inside global	Internal global address and port number
Inside local	Internal local address and port number
Outside local	External local address and port number
Outside global	External global address and port number
timeout	Time (in seconds) left before this NAT entry times out

## Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears the NAT entry table.
<b>ip nat</b>	Performs NAT on the traffic that passes this interface.
<b>ip nat inside destination</b>	Enables NAT for internal destination addresses.
<b>ip nat inside source</b>	Enables NAT for internal source addresses.
<b>ip nat outside source</b>	Enables NAT for external source addresses.
<b>ip nat pool</b>	Defines the IP NAT address pool.
<b>show ip nat translations</b>	Displays IP NAT entries.

## Platform Description

N/A

# 1 DHCP Commands

## 1.1 address range

Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the **no** form of this command to restore the default setting.

**address range** *low-ip-address high-ip-address*

**no address range**

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Start address in the network segment range.
	<i>high-ip-address</i>	End address in the network segment range.

**Defaults** By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.

**Command Mode** Address pool CLASS configuration mode.

**Usage Guide** Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSES. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.

**Configuration Examples** The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# class class1
Hostname(config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8

```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	<b>class</b>	Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode.

**Platform Description** N/A

## 1.2 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

**bootfile** *file-name*

**no bootfile**

**default bootfile**

Parameter	Parameter	Description
Description	<i>file-name</i>	Startup file name.

**Defaults** No startup file name is defined by default.

**Command** DHCP address pool configuration mode

**Mode**

**Usage Guide** Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

**Configuration** The following example defines the device.conf as the startup file name.

**Examples**

```
Hostname(config)#ip dhcp pool mypool1
Hostname(dhcp-config)#bootfile device.conf
```

Related	Command	Description
<b>Commands</b>	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>next-server</b>	Configures the next server IP address of the DHCP client startup process.

**Platform** N/A

**Description**

## 1.3 class

Use this command to configure the associated CLASS in the DHCP address pool. Use the **no** form of this command to restore the default setting.

**class** *class-name*

**no class**

Parameter	Parameter	Description
Description	<i>class-name</i>	Class name, which can be the character string or numeric such as myclass or 1.

**Defaults** By default, no CLASS is associated with the address pool.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSES, and each CLASS can specify different network segment range.

During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSES in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSES are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same as the range of address pool where the CLASS is.

**Configuration Examples** The following example configures the address *mypool0* to associate with class1.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# class class1

```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

## 1.4 clear ip dhcp binding

Use this command to clear the DHCP binding table in the privileged user mode.

```
clear ip dhcp binding { * | ip-address }
```

Parameter Description	Parameter	Description
	*	Deletes all DHCP bindings.
	<i>ip-address</i>	Deletes the binding of the specified IP addresses.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the **no ip dhcp pool** command.

**Configuration** The following example clears the DHCP binding with the IP address 192.168.12.100.

**Examples**

```
Hostname# clear ip dhcp binding 192.168.12.100
```

Related Commands	Command	Description
	<b>show ip dhcp binding</b>	Displays the address binding of the DHCP server.

**Platform Description** N/A

## 1.5 clear ip dhcp conflict

Use this command to clear the DHCP address conflict record.

**clear ip dhcp conflict** { \* | *ip-address* }

Parameter Description	Parameter	Description
	*	Deletes all DHCP address conflict records.
	<i>ip-address</i>	Deletes the conflict record of the specified IP addresses.

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The **clear ip dhcp conflict** command can be used to delete the history conflict record.

**Configuration** The following example clears all address conflict records.

**Examples**

```
Hostname# clear ip dhcp conflict *
```

Related Commands	Command	Description
	<b>ip dhcp ping packets</b>	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	<b>show ip dhcp conflict</b>	Displays the address conflict that the DHCP server detects when it assigns an IP address.

**Platform** N/A

**Description**

## 1.6 clear ip dhcp history

Use this command to clear the address assigned by the DHCP server.

**clear ip dhcp history** { \* | *mac-address* }

Parameter	Parameter	Description
<b>Description</b>	*	Clears all addresses assigned by the DHCP server.
	<i>mac-address</i>	Clears the address assigned by the DHCP server corresponding to the specified MAC address.

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example clears all addresses assigned by the DHCP server.

**Examples**

```
Hostname# clear ip dhcp history *
```

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A

**Description**

## 1.7 clear ip dhcp server detect

Use this command to clear statistics about the fake DHCP server.

**clear ip dhcp server detect** { \* | *ip-address* }

Parameter	Parameter	Description
<b>Description</b>	*	Clears statistics about all fake DHCP servers.
	<i>ip-address</i>	Clears statistics about the specified fake DHCP server.

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** The detected fake DHCP server addresses are saved on the server. You can use the **clear ip dhcp server detect** command to clear statistics about the fake DHCP server.

**Configuration** The following example clears statistics about all fake DHCP servers.

**Examples**

```
Hostname# clear ip dhcp server detect *
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.8 clear ip dhcp server rate

Use this command to clear statistics about the packet processing rate of every module.

**clear ip dhcp server rate**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.

**Configuration** The following example clears statistics about the packet processing rate of every module.

**Examples**

```
Hostname# clear ip dhcp server rate
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 clear ip dhcp server statistics

Use this command to reset the counter of the DHCP server in the privileged user mode.

**clear ip dhcp server statistics**

Parameter	Parameter	Description
-----------	-----------	-------------



<b>Description</b>	N/A	N/A				
<b>Defaults</b>	N/A					
<b>Command Mode</b>	Privileged EXEC mode.					
<b>Usage Guide</b>	The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The <b>clear ip dhcp server statistics</b> command can be used to delete the history counter record and carry out the statistics starting from scratch.					
<b>Configuration</b>	The following example clears the statistics record of the DHCP server.					
<b>Examples</b>	<pre>Hostname# clear ip dhcp server statistics</pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show ip dhcp server statistics</b></td> <td>Displays the statistics record of the DHCP server.</td> </tr> </tbody> </table>	Command	Description	<b>show ip dhcp server statistics</b>	Displays the statistics record of the DHCP server.	
Command	Description					
<b>show ip dhcp server statistics</b>	Displays the statistics record of the DHCP server.					
<b>Platform Description</b>	N/A					

## 1.10 clear ip dhcp relay statistics

Use this command to clear the DHCP relay statistics.

**clear ip dhcp relay statistics**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	The DHCP relay is configured with the counter to count various packets received or transmitted by the relay. This command is used to clear the counters.				
<b>Configuration</b>	The following example clears the DHCP relay statistics.				
<b>Examples</b>	<pre>Hostname# clear ip dhcp relay statistics</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				

**Platform** N/A

**Description**

## 1.11 client-identifier

Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**client-identifier** *unique-identifier*

**no client-identifier**

**default client-identifier**

Parameter	Parameter	Description
<b>Description</b>	<i>unique-identifier</i>	The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

**Defaults** N/A.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media.

The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700. This command is used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# client-identifier 00d0.f822.33b4

```

Related Commands	Command	Description
	<b>hardware-address</b>	Defines the hardware address of DHCP client.
	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.12 client-name

Use this command to define the name of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**client-name** *client-name*

**no client-name**

**default client-name**

Parameter	Parameter	Description
<b>Description</b>	client-name	Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.

**Defaults** No client name is defined by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.

**Configuration** The following example defines a string river as the name of the client.

```

Examples
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# client-name river

```

Related	Command	Description
<b>Commands</b>	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.13 default-router

Use this command to define the default gateway of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**default-router** *ip-address* [ *ip-address2*...*ip-address8* ]

**no default-router**  
**default default-route**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the equipment. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 gateways can be configured.

**Defaults** No gateway is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.

**Configuration Examples** The following example defines 192.168.12.1 as the default gateway.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# default-router 192.168.12.1

```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform Description** N/A

## 1.14 dns-server

Use this command to define the DNS server of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**dns-server** { *ip-address* [ *ip-address2...ip-address8* ] }  
**no dns-server**  
**default dns-server**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the DNS server. At least one IP address should be configured.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 DNS servers can be configured.

**Defaults** No DNS server is defined by default.

**Command** DHCP address pool configuration mode.  
**Mode**

**Usage Guide** When more than one DNS server is defined, the former will possess higher priority, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails. If the RGOS software also acts as the DHCP client, the DNS server information obtained by the client can be transmitted to the DHCP client.

**Configuration** The following example specifies the DNS server 192.168.12.3 for the DHCP client.

**Examples**

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# dns-server 192.168.12.3

```

Related Commands	Command	Description
	<b>domain-name</b>	Defines the suffix domain name of the DHCP client.
	<b>ip address dhcp</b>	Enables the DHCP client on the interface to obtain the IP address information.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A  
**Description**

## 1.15 domain-name

Use this command to define the suffix domain name of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**domain-name** *domain-name*

**no domain-name**

**default domain-name**

Parameter	Parameter	Description
<b>Description</b>	<i>domain-name</i>	Defines the suffix domain name string of the DHCP client.

**Defaults** No suffix domain name by default.

**Command** DHCP address pool configuration mode.  
**Mode**

**Usage Guide** After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.

**Configuration** The following example defines the suffix domain name i-net.com.cn for the DHCP client.

**Examples**

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# domain-name test.com.cn

```

Related	Command	Description
Commands	<b>dns-server</b>	Defines the DNS server of the DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.16 force-no-router

Use this command to cancel gateway allocation to the client. Use the **no** or **default** form of this command to restore the default setting.

**force-no-router**

**no force-no-router**

**default force-no-router**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command** DHCP address pool configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example cancels gateway allocation to the client.

```

Examples
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# force-no-router

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.17 hardware-address

Use this command to define the hardware address of the DHCP client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**hardware-address** *hardware-address* [ *type* ]

**no hardware-address**

**default hardware-address**

Parameter	Parameter	Description
Description	<i>hardware-address</i>	Define the MAC address of the DHCP client.
	<i>type</i>	To indicate the hardware platform protocol of the DHCP client, use the string definition or digits definition. String option: Ethernet ieee802 Digits option: 1 (10M Ethernet) 6 (IEEE 802)

**Defaults** No hardware address is defined by default.  
If there is no option when the hardware address is defined, it is the Ethernet by default.

**Command** DHCP address pool configuration mode.  
**Mode**

**Usage Guide** This command can be used only when the DHCP is defined by manual binding.

**Configuration** The following example defines the MAC address 00d0.f838.bf3d with the type ethernet.

**Examples**

```

Hostname(config)# ip dhcp pool mypool10
Hostname(dhcp-config)# hardware-address 00d0.f838.bf3d

```

Related Commands	Command	Description
	<b>client-identifier</b>	Defines the unique ID of the DHCP client (Indicated by the hexadecimal numeral, separated by dot).
	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>default-router</b>	Defines the default route of the DHCP client.

**Platform** N/A  
**Description**

## 1.18 host

Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**host** *ip-address* [ *netmask* ]

**no host**  
**default host**

Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of DHCP client.
	<i>netmask</i>	Defines the network mask of DHCP client.

**Defaults** No IP address or network mask of the host is defined.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address.  
 This command can be used only when the DHCP is defined by manual binding.

**Configuration Examples** The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# host 192.168.12.91 255.255.255.240
  
```

Related Commands	Command	Description
default-router	<b>client-identifier</b>	Defines the unique ID of the DHCP client (Indicated in hex and separated by dot).
	<b>hardware-address</b>	Defines the hardware address of DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	Define the default route of the DHCP client.	<b>default-router</b>

**Platform** N/A

**Description**

## 1.19 ip address dhcp

Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip address dhcp**

**no ip address dhcp**

**default ip address dhcp**



Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The interface cannot obtain the IP address by the DHCP by default.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** When requesting the IP address, the DHCP client of the RGOS software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional).

The client of the RGOS software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server.

**Configuration** The following example makes the BVI 1 port obtain the IP address automatically.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip address dhcp

```

Related	Command	Description
Commands	<b>dns-server</b>	Defines the DNS server of DHCP client.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.20 ip dhcp class

Use this command to define a CLASS and enter the global CLASS configuration mode. Use the **no** form of this command to restore the default setting.

**ip dhcp class** *class-name*

**no ip dhcp class** *class-name*

Parameter	Parameter	Description
Description	<i>class-name</i>	Class name, which can be character string or numeric such as myclass or 1.

**Defaults** By default, the class is not configured.

**Command** Global configuration mode.

**Mode**

**Usage Guide** After executing this command, it enters the global CLASS configuration mode which is shown as “Ruijie (config-dhcp-class)#”. In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.

**Configuration** The following example configures a global CLASS.

**Examples**

```

Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)#

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.21 ip dhcp client class-id

Use this command to define the class-id field in the request messages sent from DHCP clients. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp client class-id { ascii | hex } string**

**no ip dhcp client class-id**

**default ip dhcp client class-id**

Parameter	Parameter	Description
<b>Description</b>	<i>hex</i>	Hexadecimal format.
	<i>ascii</i>	ASCII code.
	<i>string</i>	Content of the class-id string.

**Defaults** By default, the string content is vendor-specific.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is run on DHCP clients.

**Configuration** The following example defines the class-id field as test.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp client class-id ascii test

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.22 ip dhcp client client-id

Use this command to define the client-id field in the request messages sent from DHCP clients. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp client client-id { *ascii string* | *hex string* | **exclude interface-name** }**

**no ip dhcp client client-id**

**default ip dhcp client client-id**

Parameter	Parameter	Description
Description	<i>hex</i>	Hexadecimal format.
	<i>ascii</i>	ASCII code.
	<i>string</i>	Content of the client-id string.
	<b>exclude interface-name</b>	Excluding interface name.

**Defaults** The default content of the client-id field is: interface type + MAC address + interface name

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is run on DHCP clients.

**Configuration** The following example defines the client-id field as 0102.0304.0506.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp client client-id hex 0102.0304.0506

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.23 ip dhcp client hostname

Use this command to define the hostname field in the request messages sent from DHCP clients. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp client hostname *string***

**no ip dhcp client hostname**

**default ip dhcp client hostname**

Parameter	Parameter	Description
Description	<i>string</i>	Content of the hostname string.

**Defaults** By default, the string content is the hostname.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is run on DHCP clients.

**Configuration** The following example defines the hostname as Hostname.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp client hostname Hostname
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.24 ip dhcp client lease

Use this command to define the lease field in the request messages sent from DHCP clients. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp client lease** *days* [ *hours* ] [ *minutes* ]

**no ip dhcp client lease**

**default ip dhcp client lease**

Parameter Description	Parameter	Description
	<i>days</i>	Lease time in the unit of day.
	<i>hours</i>	(Optional) Lease time in the unit of hour. This parameter can be defined after <i>day</i> is configured. Its default value is 0.
	<i>minutes</i>	(Optional) Lease time in the unit of minute. This parameter can be defined after <i>day</i> and <i>minutes</i> are configured. Its default value is 0.

**Defaults** By default, no content is configured for the lease field.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is run on DHCP clients.

**Configuration** The following example sets the lease time to one hour. .

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp client lease 0 1
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A  
**Description**

## 1.25 ip dhcp client option-list include

Use this command to define the option-list field in the request messages sent from DHCP clients. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp client option-list include** *string*

**no ip dhcp client option-list include**

**default ip dhcp client option-list include**

Parameter	Parameter	Description
Description	<i>string</i>	String content of the option-list field.

**Defaults** By default, only mandatory content is included in the option-list field.

**Command Mode** Interface configuration mode.

**Usage Guide** This command is run on DHCP clients.

**Configuration** The following example defines the option-list as 66, 67, 43.

```

Examples
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp client option-list include 66-67,43

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A  
**Description**

## 1.26 ip dhcp excluded-address

Use this command to define some IP addresses and make the DHCP server not assign them to the DHCP client in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

**no ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

**default ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

Parameter	Parameter	Description
Description	<i>low-ip-address</i>	Excludes the IP address, or excludes the start IP address within the range of the IP address.
	<i>high-ip-address</i>	Excludes the end IP address within the range of the IP address.

**Defaults** The DHCP server assigns the IP addresses of the whole address pool by default.

**Command Mode** Global configuration mode.

**Usage Guide** If the excluded IP address is not configured, the DHCP server attempts to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts to prevent these addresses are assigned to the DHCP client, and define the excluded IP address accurately to reduce the conflict detecting time when the DHCP server assigns the address.

**Configuration Examples** In the following example, the DHCP server will not attempt to assign the IP addresses within 192.168.12.100~150.

```
ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

The following example restores the default setting.

```
Hostname(config)# no ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	<b>network (DHCP)</b>	Defines the network number and network mask of the DHCP address pool.

**Platform** N/A

**Description**

## 1.27 ip dhcp force-send-nak

Use this command to configure the forcible NAK packet sending function. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp force-send-nak**

**no ip dhcp force-send-nak**

**default ip dhcp force-send-nak**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** The DHCP client checks the previously used IP address every time it is started and sends a DHCP Request packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCP Discover packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCP Discover packets. The forcible NAK packet sending function is added to shorten the interval at which the client sends DHCP Discover packets.

**Configuration Examples** The following example enables the forcible NAK packet sending function in global configuration mode.

```
Hostname(config)# ip dhcp force-send-nak
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.28 ip dhcp monitor-vrrp-state

Use this command in layer-3 configuration mode to enable the DHCP Server to monitor the status of VRRP interfaces so that the DHCP Server processes only those packets sent from a VRRP interface in the Master state. Use the **no** or **default** form of this command to restore the default setting. If it is canceled, the DHCP Server processes packets from VRRP interfaces in the Master or Backup state.

**ip dhcp monitor-vrrp-state**  
**no ip dhcp monitor-vrrp-state**  
**default ip dhcp monitor-vrrp-state**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The **ip dhcp monitor-vrrp-state** command is disabled by default. .

**Command Mode** Interface configuration mode.

**Usage Guide** If a VRRP address is configured for an interface, the DHCP Server processes packets sent from the master interface and discards packets sent from the backup interface. If no VRRP address is configured, the DHCP Server does not monitor the status of VRRP interfaces. All DHCP packets will

be processed.

**Configuration** The following example enables the DHCP Server to monitor the status of VRRP interfaces.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1) ip dhcp monitor-vrrp-state
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.29 ip dhcp ping packets

Use this command to configure the times of pinging the IP address when the DHCP server detects address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp ping packets** [ *number* ]

**no ip dhcp ping packets**

**default ip dhcp ping packets**

Parameter	Parameter	Description
Description	<i>number</i>	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.

**Defaults** The Ping operation sends two packets by default.

**Command Mode** Global configuration mode.

**Usage Guide** When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.

**Configuration** The following example sets the number of the packets sent by the ping operation as 3.

**Examples**

```
Hostname(config)# ip dhcp ping packets 3
```

Related	Command	Description
Commands	<b>clear ip dhcp conflict</b>	Clears the DHCP history conflict record.
	<b>ip dhcp ping packet</b>	Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned.



	Otherwise, it will record the address conflict.
<b>show ip dhcp conflict</b>	Displays the DHCP server detects address conflict when it assigns an IP address.

**Platform** N/A

**Description**

### 1.30 ip dhcp ping timeout

Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp ping timeout** *milli-seconds*

**no ip dhcp ping timeout**

**default ip dhcp ping timeout**

Parameter	Parameter	Description
<b>Description</b>	<i>milli-seconds</i>	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

**Defaults** The default is 500 seconds.

**Command** Global configuration mode.

**Mode**

**Usage Guide** This command defines the time that the DHCP server waits for a ping response packet.

**Configuration** The following example configures the waiting time of the ping response packet to 600ms.

**Examples**

```
Hostname(config)# ip dhcp ping timeout 600
```

Related	Command	Description
<b>Commands</b>	<b>clear ip dhcp conflict</b>	Clears the DHCP history conflict record.
	<b>ip dhcp ping packets</b>	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	<b>show ip dhcp conflict</b>	Displays the address conflict the DHCP server detects when it assigns an IP address.

**Platform** N/A

**Description**

## 1.31 ip dhcp pool

Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp pool** *pool-name*

**no ip dhcp pool** *pool-name*

**default ip dhcp pool** *pool-name*

Parameter	Parameter	Description
Description	<i>pool-name</i>	A string of characters and positive integers, for instance, mypool or 1.

**Defaults** No DHCP address pool is defined by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** Execute the command to enter the DHCP address pool configuration mode:

```
Hostname(dhcp-config)#
```

In this configuration mode, configure the IP address range, the DNS server and the default gateway.

**Configuration** The following example defines a DHCP address pool named mypool0.

**Examples**

```
Hostname(config)# ip dhcp pool mypool0
```

```
Hostname(dhcp-config)#
```

Related Commands	Command	Description
	<b>host</b>	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	<b>ip dhcp excluded-address</b>	Defines the IP addresses that the DHCP server cannot assign to the clients.
	<b>network (DHCP)</b>	Defines the network number and network mask of the DHCP address pool.

**Platform** N/A

**Description**

## 1.32 ip dhcp refresh arp

Use this command to refreshes the trusted ARP allocation.

**ip dhcp refresh arp**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	N/A	N/A				
<b>Defaults</b>	N/A					
<b>Command Mode</b>	Global configuration mode					
<b>Usage Guide</b>	This command is configured on the DHCP server.					
<b>Configuration Examples</b>	The following example refreshes the trusted ARP allocation.					
<b>Examples</b>	<pre>Hostname(config)#ip dhcp refresh arp</pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
<b>Platform Description</b>	N/A					

### 1.33 ip dhcp relay check server-id

Use this command to enable the DHCP relay agent to forward DHCP request packets to the specified DHCP server. Use the **no** form of this command to restore the default setting.

**ip dhcp relay check server-id**  
**no ip dhcp relay check server-id**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	The <b>ip dhcp relay check server-id</b> command is disabled.				
<b>Command Mode</b>	Global configuration mode.				
<b>Usage Guide</b>	This is a DHCP relay feature. After this command is configured, the DHCP relay agent forwards DHCP request packets to only the specified DHCP server. Otherwise, the DHCP requests packets are forwarded to all DHCP servers.				
<b>Configuration Examples</b>	<p>The following example enables the ip dhcp relay check server-id function.</p> <pre>Hostname# configure terminal Hostname(config)# ip dhcp relay check server-id</pre> <p>The following example disables the ip dhcp relay check server-id function.</p> <pre>Hostname(config)# no ip dhcp relay check server-id</pre>				

Related	Command	Description
Commands	<b>service dhcp</b>	Enables the DHCP Relay.

**Platform** N/A

**Description**

## 1.34 ip dhcp relay information circuit-id string

Use this command to configure the device name in the circuit ID of option 82. Use the **no** form of this command to restore the default setting.

**ip dhcp relay information circuit-id string** [ *devicename* ]

**no ip dhcp relay information option82**

Parameter	Parameter	Description
Description	<i>devicename</i>	Configures the device name.

**Defaults** No device name in the circuit ID of option 82 is configured by default.

**Command** Global configuration mode

**Mode**

**Default Level** 14

**Usage Guide** This is a DHCP relay feature. After this command is configured, the DHCP relay agent adds the circuit-id field of option 82 to DHCP request packets during packet forwarding.

**Configuration Examples** The following example configures the device name in the circuit ID of option 82.

```
Hostname(config)# ip dhcp relay information circuit-id string device-name
```

The following example removes the device name from the circuit ID of option 82.

```
Hostname(config)# no ip dhcp relay information circuit-id string
```

**Verification** Run the **show running-config** command to check the configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.35 ip dhcp relay information option82

Use this command to enable the **ip dhcp relay information option82** function. Use the **no** form of this command to restore the default setting.

**ip dhcp relay information option82 [ standard-format | verbose-format ]**

**no ip dhcp relay information option82 [ standard-format | verbose-format ]**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ip dhcp relay information option82** command is disabled.

**Command Mode** Global configuration mode.

**Usage Guide** This is a DHCP relay feature.

After the **ip dhcp relay information option82** command is configured, the DHCP relay agent adds option 82 to DHCP request packets during packet forwarding. The encapsulation format for the circuit-id field of option 82 is slot(1):port(1):dev\_name(<=64) and that of the remote-id field is user\_mac(6):iftype(1):port\_name(<=64):vid(2).

After the **ip dhcp relay information option82 standard-format** command is configured, the DHCP relay agent adds option 82 to DHCP request packets during packet forwarding. The encapsulation format for the circuit-id field of option 82 is vid(2):slot(1):port(1) and that of the remote-id field is sys\_mac(6).

After the **ip dhcp relay information option82 verbose-format** command is configured, the DHCP relay agent adds option 82 to DHCP request packets during packet forwarding. The encapsulation format for the circuit-id field of option 82 is mac port\_name vid (with each field separated by spaces) and that of the remote-id field is hostname.

The preceding three commands are mutually exclusive. Only one among them is active. When you remove an encapsulation command, DHCP option 82 is disabled.

**Configuration Examples** The following example enables the option82 function on the DHCP relay.

```
Hostname# configure terminal
Hostname(config)# ip dhcp relay information option82
```

The following example disables the option82 function on the DHCP relay.

```
Hostname(config)# no ip dhcp relay information option82
```

Related Commands	Command	Description
	<b>service dhcp</b>	Enables the DHCP Relay.

**Platform Description** N/A

## 1.36 ip dhcp server detect

Use this command to enable the fake DHCP server detection. Use the **no** or **default** form of this command to restore the default setting.

**ip dhcp server detect**

**no ip dhcp server detect**

**default ip dhcp server detect**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After this function is enabled, any fake DHCP server detected is logged.

**Configuration Examples** The following example enables the fake DHCP server detection.

```
Hostname(config)# ip dhcp server detect
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.37 ip dhcp use class

Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the **no** form of this command can be used to disable the CLASS.

**ip dhcp use class**

**no ip dhcp use class**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** Enabled

**Command Mode** Global configuration mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example enables the CLASS to allocate addresses.

**Examples**

```
Hostname(config)# ip dhcp use class
```

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A

**Description**

## 1.38 ip helper-address

Use this command to add an IP address of the DHCP server. Use the **no** form of this command to delete an IP address of the DHCP server.

The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.

**ip helper-address** { **cycle-mode** | *A.B.C.D* }

**no ip helper-address** { **cycle-mode** | *A.B.C.D* }

Parameter	Parameter	Description
<b>Description</b>	<b>cycle-mode</b>	Forwards DHCP request packets to all DHCP servers. This parameter is not supported by some interface configuration modes, which is subject to the actual situation.
	<i>A.B.C.D</i>	The IP address of the specified DHCP server.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** This is a DHCP relay feature. After the DHCP server is configured with an IP address, the DHCP relay agent forwards DHCP request packets to the DHCP server and DHCP reply packets to the DHCP client.

The DHCP server IP address can be configured either globally or on a Layer 3 interface. Up to 20 DHCP server addresses can be configured globally or on each Layer 3 interface. When an interface receives a DHCP request packet, the DHCP server list on the interface applies first. If the interface is not configured with a DHCP server list, the global DHCP server list takes effect.

In global configuration mode, the cycle-mode parameter can be configured for the DHCP relay agent. If cycle-mode is configured, the DHCP relay agent forwards packets from DHCP clients to all DHCP servers matching the preceding rule. If cycle-mode is not configured, the DHCP relay agent forwards packets from DHCP clients to only the first DHCP server matching the preceding rule. Cycle-mode is configured only in global configuration mode but applies to both global and interface configuration modes. Cycle-mode is enabled by default.

**Configuration** The following example configures IP address 192.168.11.1 for the DHCP server on interface bvi 1.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ip helper-address 192.168.11.1

```

The following example removes IP address 192.168.11.1 from the DHCP server on interface bvi 1.

```

Hostname(config-if-BVI 1)# no ip helper-address 192.168.11.1

```

The following example sets the IP address for the global server to 192.168.100.1

```

Hostname# configure terminal
Hostname(config)# ip helper-address 192.168.100.1

```

The following example deletes the set IP address for the global server, 192.168.100.1.

```

Hostname(config)# no ip helper-address 192.168.100.1

```

The following example enables forwarding DHCP request packets to all DHCP servers.

```

Hostname(config)# ip helper-address cycle-mode

```

The following example disables forwarding DHCP request packets to all DHCP servers.

```

Hostname(config)# no ip helper-address cycle-mode

```

**Related  
Commands**

Command	Description
<b>service dhcp</b>	Enables the DHCP relay.

**Platform  
Description**

N/A

## 1.39 lease

Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.

**lease** { *days* [ *hours* ] [ *minutes* ] | **infinite** }

**no lease**

**default lease**

**Parameter  
Description**

Parameter	Description
<i>days</i>	Lease time in days
<i>hours</i>	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
<i>minutes</i>	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.



<b>infinite</b>	Infinite lease time.
-----------------	----------------------

**Defaults** The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.

**Configuration** The following example sets the DHCP lease to 1 hour.

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease 0 1
```

The following example sets the DHCP lease to 1 minute.

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease 0 0 1
```

Related Commands	Command	Description
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.40 lease-threshold

Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold.

Use the **default** or **no** form of this command to restore the default setting.

**lease-threshold** *percentage*

**default lease-threshold**

**no lease-threshold**

Parameter Description	Parameter	Description
	<i>percentage</i>	Usage of the address pool, ranging from 60 to 100 in percentage.

**Defaults** 90

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total

number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.

**Configuration** The following example sets the alarm threshold to 80%.

**Examples**

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# lease-threshold 80
```

The following example restores the default alarm threshold.

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# default lease-threshold
```

**Related  
Commands**

Command	Description
<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.41 netbios-name-server

Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The **no** or **default** form of this command can be used to restore the default setting.

**netbios-name-server** *ip-address* [ *ip-address2...ip-address8* ]

**no netbios-name-server**

**default netbios-name-server**

**Parameter  
Description**

Parameter	Description
<i>ip-address</i>	IP address of the WINS server. It is required to configure one IP address at least.
<i>ip-address2...ip-address8</i>	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.

**Defaults** No WINS server is defined by default.

**Command  
Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one WINS server is defined, the former has higher priority. The DHCP client will select the next WINS server only when its communication with the former WINS server fails.

**Configuration** The following example specifies the WINS server 192.168.12.3 for the DHCP client.

**Examples**

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# netbios-name-server 192.168.12.3
```

Related	Command	Description
Commands	<b>ip address dhcp</b>	Enables the DHCP client on the interface to obtain the IP address.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	<b>netbios-node-type</b>	Defines the netbios node type of the client host.

**Platform** N/A

**Description**

## 1.42 netbios-node-type

Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**netbios-node-type** *type*

**no netbios-node-type**

**default netbios-node-type**

Parameter	Parameter	Description
Description	<i>type</i>	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node m-node: mixed node h-node: hybrid node

**Defaults** No type of the NetBIOS node is defined by default.

**Command** DHCP address pool configuration mode.

**Mode**

**Usage Guide** There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution

firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received.

By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.

**Configuration** The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid.

**Examples**

```
Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# netbios-node-type h-node
```

**Related  
Commands**

Command	Description
<b>ip dhcp pool</b>	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.
<b>netbios-name-server</b>	Configures the WINS name server of the Microsoft DHCP client NETBIOS.

**Platform** N/A  
**Description**

## 1.43 network

Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**network** *net-number net-mask [ low-ip-address high-ip-address ]*

**no network**

**default network**

**Parameter  
Description**

Parameter	Description
<i>net-number</i>	Network number of the DHCP address pool
<i>net-mask</i>	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.
<i>low-ip-address</i>	Start IP address.
<i>high-ip-address</i>	End IP address.

**Defaults** No network number or network mask is defined by default.

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP

server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address.

The **show ip dhcp binding** command can be used to view the address assignment, and the **show ip dhcp conflict** command can be used to view the address conflict detection configuration.

**Configuration Examples** The following example defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# network 192.168.12.0 255.255.255.240

```

Related Commands	Command	Description
	<b>ip dhcp excluded-address</b>	Defines the IP addresses that the DHCP server cannot assign to the clients.
	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.44 next-server

Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**next-server** *ip-address* [*ip-address2*...*ip-address8*]

**no next-server**

**default next-server**

Parameter Description	Parameter	Description
	<i>ip-address</i>	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
	<i>ip-address2</i> ... <i>ip-address8</i>	(Optional) Up to 8 startup servers can be configured.

**Defaults** N/A

**Command Mode** DHCP address pool configuration mode.

**Usage Guide** When more than one startup server is defined, the former will possess higher priority. The DHCP client will select the next startup server only when its communication with the former startup server fails.

**Configuration** The following example specifies the startup server 192.168.12.4 for the DHCP client.

**Examples**

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# next-server 192.168.12.4

```

**Related  
Commands**

Command	Description
<b>bootfile</b>	Defines the default startup mapping file name of the DHCP client.
<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
<b>ip help-address</b>	Defines the Helper address on the interface.
<b>option</b>	Configures the option of the RGOS software DHCP server.

**Platform** N/A**Description**

## 1.45 option

Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

**no option**

**default option**

**Parameter  
Description**

Parameter	Description
<i>code</i>	Defines the DHCP option codes.
<b>ascii</b> <i>string</i>	Defines an ASCII string.
<b>hex</b> <i>string</i>	Defines a hex string.
<b>ip</b> <i>ip-address</i>	Defines an IP address list.

**Defaults** N/A**Command** DHCP address pool configuration mode.**Mode****Usage Guide**

The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.

**Configuration  
Examples**

The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# option 19 hex 1

```

The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16.

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0
192.168.12.16

```

Related	Command	Description
Commands	<b>ip dhcp pool</b>	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.46 pool-status

Use this command to enable or disable the DHCP address pool.

**pool-status { enable | disable }**

Parameter	Parameter	Description
Description	<b>enable</b>	Enables the address pool.
	<b>disable</b>	Disables the address pool.

**Defaults** By default, the address pool is enabled after it is configured.

**Command** DHCP address pool configuration mode

**Mode**

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example disables the address pool.

**Examples**

```

Hostname(config)# ip dhcp pool mypool0
Hostname(dhcp-config)# pool-status disable

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.47 relay agent information

Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the **no** form of this command to delete the Option82 matching information of the CLASS.

**relay agent information**

**no relay agent information**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command** Global CLASS configuration mode

**Mode**

**Usage Guide** After executing this command, it enters the Option82 matching information configuration mode which is shown as "Ruijie (config-dhcp-class-relayinfo)#".

In this configuration mode, user can configure the class matching multiple Option82 information.

**Configuration Examples** The following example configures a global CLASS and enters the Option82 matching information configuration mode.

```

Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# relay agent information
Hostname(config-dhcp-class-relayinfo)#

```

Related	Command	Description
Commands	<b>ip dhcp class</b>	Defines a CLASS and enters the global CLASS configuration mode.

**Platform** N/A

**Description**

## 1.48 relay-information hex

Use this command to enter the Option82 matching information configuration mode. Use the **no** form of this command to delete a piece of matching information.

**relay-information hex aabb.ccdd.eeff... [\* ]**

**no relay-information hex aabb.ccdd.eeff... [\* ]**

Parameter	Parameter	Description
Description	<i>aabb.ccdd.eeff...[*]</i>	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.



- Defaults** N/A
- Command Mode** Global CLASS configuration mode
- Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example configures a global CLASS which can match multiple Option82 information.

**Examples**

```

Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# relay agent information
Hostname(config-dhcp-class-relayinfo)# relay-information
hex 0102256535
Hostname(config-dhcp-class-relayinfo)# relay-information
hex 010225654565
Hostname(config-dhcp-class-relayinfo)# relay-information
hex 060225654565
Hostname(config-dhcp-class-relayinfo)# relay-information
hex 060223*

```

**Related Commands**

Command	Description
<b>ip dhcp class</b>	Defines a CLASS and enter the global CLASS configuration mode.
<b>relay agent information</b>	Enters the Option82 matching information configuration mode.

- Platform** N/A
- Description**

## 1.49 release-dhcp

Use this command to enable a DHCP client to release a DHCP lease.

**release-dhcp** *type number*

**Parameter Description**

Parameter	Description
<i>type</i>	Interface type.
<i>number</i>	Interface number.

- Defaults** N/A.
- Command Mode** Privileged EXEC mode.
- Usage Guide** This command is run on DHCP clients. After the interface addresses are released, run the **renew-dhcp** command to recover dynamic addresses or run the **no ip address dhcp** command to

start a new request for IP address.

**Configuration** The following example releases the DHCP lease of BVI 100.

**Examples**

```
Hostname# release-dhcp bvi 100
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.50 remark

Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the **no** form of this command to delete the identification.

**remark** *class-remark*

**no remark**

Parameter	Parameter	Description
<b>Description</b>	class-remark	Information used to identify the CLASS, which can be the character strings with space in them.

**Defaults** N/A.

**Command** Global CLASS configuration mode.

**Mode**

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example configures the identification information for a global CLASS.

**Examples**

```
Hostname(config)# ip dhcp class myclass
Hostname(config-dhcp-class)# remark used in #1 build
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a CLASS and enter the global CLASS configuration mode.

**Platform** N/A

**Description**

## 1.51 renew-dhcp

Use this command to renew a DHCP client's lease.

**renew-dhcp** *type number*

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<i>type</i>	Interface type.
	<i>number</i>	Interface number.
<b>Defaults</b>	N/A.	
<b>Command Mode</b>	Privilege EXEC mode.	
<b>Usage Guide</b>	This command is run on DHCP clients.	
<b>Configuration Examples</b>	The following example renews the DHCP lease of BVI 100.	
<b>Examples</b>	<pre>Hostname# renew-dhcp bvi 100</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip dhcp class</b>	Defines a CLASS and enter the global CLASS configuration mode.
<b>Platform</b>	N/A	
<b>Description</b>		

## 1.52 service dhcp

Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**service dhcp**

**no service dhcp**

**default service dhcp**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	N/A	N/A
<b>Defaults</b>	The <b>service dhcp</b> command is disabled.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.	
<b>Configuration</b>	The following example enables the DHCP server and the DHCP relay feature.	

**Examples** `Hostname(config)# service dhcp`

Related Commands	Command	Description
	<code>show ip dhcp server statistics</code>	Displays various statistics information of the DHCP server.
	<code>ip helper-address [ vrf ] A.B.C.D</code>	Adds an IP address of the DHCP server.

**Platform** N/A

**Description**

## 1.53 show dhcp lease

Use this command to display the lease information of the IP address obtained by the DHCP client.

**show dhcp lease**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** If the IP address is not defined, display the binding condition of all addresses. If the IP address is defined, display the binding condition of this IP address.

**Configuration** The following example displays the result of the show dhcp lease.

**Examples**

```

Hostname# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: GigabitEthernet 0/1
Temp sub net mask: 255.255.255.0
  DHCP Lease server: 192.168.5.70, state: 3 Bound
  DHCP transaction id: 168F
  Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
Next timer fires after: 00:04:29
Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Gi0/1

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.54 show ip dhcp binding

Use this command to display the binding condition of the DHCP address.

**show ip dhcp binding** [ *ip-address* ]

Parameter	Parameter	Description
Description	<i>ip-address</i>	(Optional) Only displays the binding condition of the specified IP addresses.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address

**Configuration** The following is the result of the show ip dhcp binding.

```

Examples
Hostname# show ip dhcp binding
Total number of clients   : 4
Expired clients           : 3
Running clients           : 1

IP address      Hardware address      Lease expiration      Type
20.1.1.1        2000.0000.2011      000 days 23 hours 59 mins  Automatic
  
```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP address to be assigned to the DHCP client.
Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.
Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
Type	The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.

Related Commands	Command	Description
	<b>clear ip dhcp binding</b>	Clears the DHCP address binding table.

**Platform** N/A  
**Description**

## 1.55 show ip dhcp conflict

Use this command to show the conflict history record of the DHCP sever.

**show ip dhcp conflict**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command can display the conflict address list detected by the DHCP server.

**Configuration** The following example displays the output result of the **show ip dhcp conflict** command.

**Examples**

```

Hostname# show ip dhcp conflict
IP address  Detection Method
192.168.12.1 Ping

```

The meaning of various fields in the show result is described as follows.

Field	Description
IP address	The IP addresses which cannot be assigned to the DHCP client.
Detection Method	The conflict detection method.

Related Commands	Command	Description
	<b>clear ip dhcp conflict</b>	Clears the DHCP conflict record.

**Platform** N/A  
**Description**

## 1.56 show ip dhcp database

Use this command to display DHCP server database status.

**show ip dhcp database**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Default Level** 14

**Usage Guide** This is a DHCP server feature. It is used to display DHCP database status.

**Configuration Examples** The following example displays status of the DHCP database.

```

Hostname# show ip dhcp database
Enable          :No
Status          :ready
Save File       :Default
Successss      :0
Failures       :0
Interval Time   :86400
    
```

Field	Description
Enable	Indicates whether the database is enabled. It is used for data recovery.
Status	The status of data recovery.
Save File	The path where data is saved.
Successss	The times of successful data saving.
Failures	The times of failed data saving.
Interval Time	The interval time for data saving.

**Verification** N/A

**Prompt** N/A

**Common Errors** N/A

## 1.57 show ip dhcp history

Use this command to display the DHCP lease history.

**show ip dhcp history**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example displays the DHCP lease history.

### Examples

```

Hostname#show ip dhcp history
Expired clients          : 3
IP address              Hardware address      Lease expiration      Vlan/Relay
10.1.1.5                2222.abcd.47ac      IDLE                  4097
10.1.1.4                2222.abcd.47ae      IDLE                  4097
10.1.1.3                2222.abcd.47ad      IDLE                  4097
Running clients         : 0
  
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.58 show ip dhcp identifier

Use this command to display the DHCP address pool ID and address usage.

**show ip dhcp identifier**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode



**Usage Guide** N/A

**Configuration** The following example displays the DHCP address pool ID and address usage.

**Examples**

```

Hostname# show ip dhcp identifier
Pool name      Identifier      Total      Distributed  Remained
-----
wwp            597455782     65533     0            65533
    
```

Pool name	Address pool name.
Identifier	Address pool ID.
Total	Total number of addresses.
Distributed	Number of allocated addresses.
Remained	Number of remained addresses.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.59 show ip dhcp pool

Use this command to display the address statistics of an address pool.

**show ip dhcp pool** [ *poolname* ]

Parameter Description	Parameter	Description
	<i>poolname</i>	(Optional) Address pool whose address statistics are to be displayed.

**Defaults**

**Command** Privileged EXEC mode.  
**Mode**

**Usage Guide** This command is configured on the DHCP server. Use this command to show the address statistics of an address pool.

**Configuration** The following example displays the output result of the **show ip dhcp pool** *poolname* command.

**Examples**

```

Hostname# show ip dhcp pool
Pool name      Total      Distributed  Remained  Percentage
-----
net20          253        11           242       4.34782
    
```

The meaning of various fields in the show result is described as follows.

Field	Description
Pool name	Address pool name
Total	Total number of assignable addresses in an address pool
Distributed	Number of assigned addresses
Remained	Number of unassigned and reusable addresses
Percentage	Address utilization of an address pool

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

**Platform** N/A

**Description**

## 1.60 show ip dhcp relay-statistics

Use this command to display the statistics of the DHCP relay.

**show ip dhcp relay-statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the statistics of the DHCP relay.

**Configuration Examples** The following example displays the statistics of the DHCP relay.

```

Hostname# show ip dhcp relay-statistics
Cycle mode                0

Message                   Count
Discover                  0
Offer                     0
Request                   0
Ack                       0
Nak                       0
Decline                   0

```

Release	0
Info	0
Bad	0
Direction	Count
Rx client	0
Rx client uni	0
Rx client bro	0
Tx client	0
Tx client uni	0
Tx client bro	0
Rx server	0
Tx server	0

The meaning of various fields in the show result is described as follows.

Field	Description
Cycle mode	Whether to allow packets to be sent to multiple DHCP servers.
Discover	The number of Discover packets.
Offer	The number of Offer packets.
Request	The number of Request packets.
Ack	The number of Ack packets.
Nak	The number of Nak packets.
Decline	The number of Decline packets.
Release	The number of Release packets.
Info	The number of Info packets.
Bad	The number of error packets.
Rx client	The number of packets received from the client.
Rx client uni	The number of unicast packets received from the client.
Rx client bro	The number of broadcast packets received from the client.
Tx client	The number of packets transmitted to the client.
Tx client uni	The number of unicast packets transmitted to the client
Tx client bro	The number of multicast packets transmitted to the client
Rx server	The number of packets received from the server.
Tx server	The number of packets transmitted to the server.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.61 show ip dhcp server detect

Use this command to display the fake DHCP server detected.

**show ip dhcp server detect**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** This command is configured on the DHCP server.

**Configuration** The following example displays the fake DHCP server detected.

**Examples**

```

Hostname# show ip dhcp server detect
The DHCP Server information:
Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.62 show ip dhcp server statistics

Use this command to display the statistics of the DHCP server.

**show ip dhcp server statistics**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** This command displays the statistics of the DHCP server.

**Configuration** The following example displays the output result of the **show ip dhcp server statistics** command.

**Examples**

```

Hostname# show ip dhcp server statistics
Address pools                2
Lease counter                4
Active Lease Counter        0
Expired Lease Counter        4
Malformed messages          0
Dropped messages            0

Message                      Received
BOOTREQUEST                  216
DHCPDISCOVER                  33
DHCPPREQUEST                  25
DHCPCDECLINE                  0
DHCPCRELEASE                  1
DHCPCINFORM                   150

Message                      Sent
BOOTREPLY                     16
DHCPOFFER                      9
DHCPACK                         7
DHCPCNAK                        0
DHCPCREQTIMES                   0
DHCPCREQSUCTIMES                0
DISCOVER-PROCESS-ERROR          0
LEASE-IN-PINGSTATE              0
NO-LEASE-RESOURCE               0
SERVERID-NO-MATCH               0
-----
recv                            0
send                            0

```

The meaning of various fields in the show result is described as follows.

Field	Description
Address pools	Number of address pools.
Automatic bindings	Number of automatic address bindings.
Manual bindings	Number of manual address bindings.
Expired bindings	Number of expired address bindings.
Malformed messages	Number of malformed messages received by the DHCP.

Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.
DHCPREQTIMES	Total number of REQUEST packets
DHCPREQSUCTIMES	Number of received DHCP request packets that are successfully processed.
DISCOVER-PROCESS-ERROR	Number of received DHCP Discover packets that are failed to be processed.
LEASE-IN-PINGSTATE	Number of leases in ping state.
NO-LEASE-RESOURCE	Number of address pools containing no assignable IP addresses.
recv	Number of Discover, Request, and Inform packets.
send	Number of reply packets that should have been sent.

Related Commands	Command	Description
	<b>clear ip dhcp server statistics</b>	Clears the DHCP server statistics.

**Platform** N/A

**Description**

## 1.63 show ip dhcp socket

Use this command to display the socket used by the DHCP server.

**show ip dhcp socket**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the socket used by the DHCP server.

```

Hostname#show ip dhcp socket
dhcp socket = 47.

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.64 show ip dhcp state ssid

Use this command to display the DHCP-assigned address bound with the specified SSID.

**show ip dhcp state ssid** [ *ssid* ]

Parameter Description	Parameter	Description
	<i>ssid</i>	The SSID to be searched.

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** The following example displays the SSID bound with DHCP-assigned address. If no SSID is specified, all SSIDs and their bound IP addresses are displayed.

**Configuration Examples** The following example displays the DHCP-assigned address bound with the specified SSID.

```

Hostname#show ip dhcp state ssid wlan_free
SSID                IP address          Hardware address    State    Expiration          Type
-----
wlan_free           192.168.110.2       0cd6.bd90.4f07     ACTIVE   000 days 23 hours 48 mins Automatic
Hostname#show ip dhcp state ssid
SSID                IP address          Hardware address    State    Expiration          Type
-----
wlan_free           192.168.110.2       0cd6.bd90.4f07     ACTIVE   000 days 23 hours 48 mins Automatic

```

**Prompt** N/A

**Platform Description** N/A

## 1.65 update arp

Use this command to enable DHCP to add trusted ARP when allocating addresses. Use the **no** or **default** form of this command to restore the default setting.

**update arp**

**no update arp**  
**default update arp**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** DHCP address pool configuration mode

**Usage Guide** This command is configured on the DHCP server. The trusted ARP has a higher priority than the dynamic ARP and cannot be overwritten.

**Configuration** The following example enables DHCP to add trusted ARP when allocating addresses.

**Examples**

```

Hostname(config)# ip dhcp pool mypool10
Hostname(dhcp-config)# update arp

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A



# 1 DHCP Snooping Commands

## 1.1 clear ip dhcp snooping binding

Use this command to delete the dynamic user information from the DHCP Snooping binding database.


**clear ip dhcp snooping binding** [ *ip* ] [ *mac* ] [ *vlan vlan-id* ] [ **interface** *interface-id* | **wlan** *wlan-id* ]

Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the user MAC address to be cleared.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ip</i>	Specifies the IP address to be cleared.
	<i>interface-id</i>	Specifies the ID of the interface to be cleared.
	<i>wlan-id</i>	Specifies the ID of the WLAN to be cleared.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear the current dynamic user information from the DHCP Snooping binding database.

 After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.

**Configuration Examples** The following example clears the dynamic database information from the DHCP Snooping binding database.

```

Hostname# clear ip dhcp snooping binding
Hostname# show ip dhcp snooping binding
Total number of bindings: 0
MacAddress IpAddress Lease(sec) Type VLAN Interface
-----

```

Related Commands	Command	Description
	<b>show ip dhcp snooping binding</b>	Displays the information of the DHCP Snooping binding database.

**Platform Description** N/A

## 1.2 ip dhcp snooping

Use this command to enable the DHCP Snooping function globally.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping**

**no ip dhcp snooping**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The **show ip dhcp snooping** command is used to display whether the DHCP Snooping function is enabled.

**Configuration Examples** The following example enables the DHCP Snooping function.

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping

```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the configuration information of DHCP Snooping.
	<b>ip dhcp snooping vlan</b>	Configures DHCP Snooping enabled VLAN.

**Platform Description** N/A

## 1.3 ip dhcp snooping bootp-bind

Use this command to enable DHCP Snooping BOOTP-bind function.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping bootp-bind**

**no ip dhcp snooping bootp-bind**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.

**Configuration** The following example enables the DHCP Snooping BOOTP-bind function.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping bootp-bind

```

**Related Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 1.4 ip dhcp snooping check-giaddr

Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the **no** form of this command to restore the default setting.

**ip dhcp snooping check-giaddr**  
**no ip dhcp snooping check-giaddr**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet.  
 After the feature is enabled, the **ip dhcp snooping verify mac-address** command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.

**Configuration** The following example enables DHCP Snooping to support the function of processing Relay requests.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping check-giaddr

```

**Related  
Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the configuration information of the DHCP Snooping.

**Platform**

N/A

**Description**

## 1.5 ip dhcp snooping clear-broadcast-flag

Use this command to enable the function of clearing the broadcast flag bit.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping clear-broadcast-flag**

**no ip dhcp snooping clear-broadcast-flag**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

This function is disabled by default.

**Command**

Global configuration mode

**Mode****Usage Guide**

After the feature is enabled, DHCP Snooping checks the broadcast flag bit for non-DHCP Relay requests. If the flag bit is 1, it clears the flag bit. When receiving responses, DHCP Snooping sets the flag bit to 1 and set Layer-2 and Layer-3 destination addresses as broadcast addresses.

**Configuration**

The following example enables the function of clearing the broadcast flag bit.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping clear-broadcast-flag

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.6 ip dhcp snooping database write-delay

Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the FLASH periodically.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping database write-delay** *time*


**no ip dhcp snooping database write-delay**

Parameter Description	Parameter	Description
	<i>time</i>	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the FLASH, in the range from 600 to 86,400 in the unit of seconds

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function writes user information into FLASH in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.

 Too fast writing will reduce FLASH durability.

**Configuration Examples** The following example sets the interval at which the device writes the user information into the FLASH to 3,600 seconds.

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-delay 3600

```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the configuration information of the DHCP Snooping.

**Platform Description** N/A

## 1.7 ip dhcp snooping database write-to-flash

Use this command to write the dynamic user information of the DHCP binding database into FLASH in real time.

**ip dhcp snooping database write-to-flash**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to write the dynamic user information of the DHCP binding database into FLASH in real time.  
Wireless user information is not written to FLASH.

If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored because the two versions correspond to different FLASHs.

**Configuration Examples** The following example writes the dynamic user information of the DHCP binding database into FLASH.

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-to-flash

```

Related Commands	Command	Description
		N/A

**Platform Description** N/A

## 1.8 ip dhcp snooping information option

Use this command to add Option82 to the DHCP request message.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping information option [ standard-format | format ]**

**no ip dhcp snooping information option [ standard-format | format ]**

Parameter Description	Parameter	Description
	<b>standard-format</b>	The standard format.
	<b>format</b>	The DHCP information option format.


**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command adds Option82 to the DHCP request messages based on which the DHCP server assigns IP addresses.

By default, this function is in extended mode.

 DHCP Relay function adds Option82 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping Option82 and DHCP Relay at the same time.

**Configuration** The following example adds Option82 to the DHCP request message.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option
Hostname(config)# end

```

**Related Commands**

Command	Description
<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 1.9 ip dhcp snooping information option format remote-id

Use this command to set the Option82 sub-option remote-id as the customized character string.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping information option format remote-id { string *ascii-string* | hostname }**

**no ip dhcp snooping information option format remote-id { string *ascii-string* | hostname }**

**Parameter Description**

Parameter	Description
<b>string</b> <i>ascii-string</i>	The content of the Option82 remote-id extension format is customized character string.
<b>hostname</b>	The content of the Option82 remote-id extension format hostname

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command sets the remote-id in the Option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the Option82 information.

**Configuration** The following example adds the Option82 into the DHCP request packets with the content of

**Examples** remote-id as hostname.

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping information option format remote-id
hostname

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.10 ip dhcp snooping suppression

Use this command to set the port to be the suppression status.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping suppression**

**no ip dhcp snooping suppression**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command  
Mode** dot11 radio interface mode or WLAN security configuration mode

**Usage Guide** This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP.  
This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

**Configuration** The following example sets GigabitEthernet 0/1 and WLAN 1 to be in the suppression status.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping suppression
Hostname(config-if-GigabitEthernet 0/1)# end
Hostname# configure terminal
Hostname(config)# wlansec 1
Hostname(config-wlansec)# ip dhcp snooping suppression
Hostname(config-if-wlansec)# end

```

**Related**

Command	Description
---------	-------------



Commands	
<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 1.11 ip dhcp snooping trust

Use this command to set the trusted ports for DHCP Snooping.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** All ports are untrusted by default.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).

**Configuration Examples** The following example sets GigabitEthernet 0/1 as a trusted port:

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping trust

```

Related Commands	Command	Description
	<b>show ip dhcp snooping</b>	Displays the DHCP Snooping configuration.

**Platform** N/A

**Description**

## 1.12 ip dhcp snooping verify mac-address

Use this command to check whether the source MAC address of the DHCP request message matches against the **client addr** field of the DHCP message.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

Parameter Description	Parameter	Description
		N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.

**Configuration Examples** The following example enables the check of the source MAC address of the DHCP request message.

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping verify mac-address

```

Related Commands	Command	Description
		<b>show ip dhcp snooping</b>

**Platform Description** N/A

## 1.13 ip dhcp snooping vlan

Use this command to enable DHCP Snooping for the specific VLAN.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping vlan** { *vlan-rng* | { *vlan-min* [ *vlan-max* ] } }

**no ip dhcp snooping vlan** { *vlan-rng* | { *vlan-min* [ *vlan-max* ] } }

Parameter Description	Parameter	Description
		<i>vlan-rng</i>
	<i>vlan-min</i>	Minimum VLAN of effective DHCP Snooping
	<i>vlan-max</i>	Maximum VLAN of effective DHCP Snooping

**Defaults** By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to enable DHCP Snooping for specified VLANs globally.

**Configuration** The following example enables the DHCP Snooping function in VLAN 1000.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip dhcp snooping vlan 1000

```

**Related  
Commands**

Command	Description
<b>ip dhcp snooping</b>	Enables DHCP Snooping globally.

**Platform** N/A

**Description**

## 1.14 ip dhcp snooping vlan information option change-vlan-to vlan

Use this command to enable the Option82 sub-option circuit-id and change the VLAN in the circuit-id into the specified VLAN.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id***

**no ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id***

**Parameter  
Description**

Parameter	Description
<i>vlan-id</i>	The ID of the VLAN to be replaced

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** With this command configured, the Option82 is added to the DHCP request packets, the circuit-id in the Option82 information is the specified VLAN and the DHCP server will assign the addresses according to the Option82 information.

**Configuration** The following adds the Option82 to the DHCP request packets and changes the VLAN 4094 in the Option82 sub-option circuit-id to VLAN 4093:

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094
information option change-vlan-to vlan 4093

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.15 ip dhcp snooping vlan information option format-type circuit-id string

Use this command to configure the Option82 sub-option circuit-id as user-defined (the storage format is ASCII) and to perform the packet forwarding.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

**no ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

Parameter Description	Parameter	Description
	<i>vlan-id</i>	
<i>ascii-string</i>		The user-defined content to fill to the Circuit ID

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to add the Option82 to the DHCP request packets. The content of the sub-option circuit-id is customized with 3 to 63 bytes, and the DHCP server will assign the addresses according to the Option82 information.

**Configuration Examples** The following example adds the Option82 to the DHCP request packets with the content of the sub-option circuit-id as *port-name*.

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094
information option format-type circuit-id string port-name

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.16 ip dhcp snooping vlan max-user

Use this command to set the maximum number of users bound with the VLAN.

Use the **no** form of this command to restore the default setting.

**ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*

**no ip dhcp snooping vlan** *vlan-word* **max-user** *user-number*

Parameter Description	Parameter	Description
	<i>vlan-word</i>	The VLAN range
	<i>user-number</i>	The maximum number of users bound with the VLAN

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** Use this command to set the maximum number of users bound with the VLAN. This function combined with the corresponding topology can prevent illegal DHCP packet attacks.

**Configuration Examples** The following example sets the maximum number of users bound with VLAN 1 to 10 and VLAN 20 to 30 respectively.

```

Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20
max-user 30

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.17 renew ip dhcp snooping database

Use this command to import the information in current backup file to the DHCP Snooping binding database manually as needed.

**renew ip dhcp snooping database**


Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to import the backup file information to the DHCP Snooping database in real time.

 Records out of lease time and repeated will be neglected.

**Configuration** The following example imports the backup file information to the DHCP Snooping database.

**Examples** Hostname# renew ip dhcp snooping database

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.18 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

**show ip dhcp snooping**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the DHCP Snooping configuration.

**Examples** Hostname# show ip dhcp snooping  
Switch DHCP snooping status :ENABLE  
Verification of hwaddr field status :DISABLE  
DHCP snooping database write-delay time: 0 seconds

```
DHCP snooping option 82 status: ENABLE
DHCP snooping Support Bootp bind status: ENABLE
Interface                               Trusted                               Rate
limit (pps)
-----                               -----
GigabitEthernet 0/1                     YES                               unlimited
Default                                  No
```

Field	Description
Switch DHCP snooping status	Indicates whether DHCP Snooping is enabled globally.
Verification of hwaddr field status	Indicates whether source MAC check is enabled.
DHCP snooping database write-delay time	Interval for writing data to a backup file.
DHCP snooping option 82 status	Indicates whether Option 82 is added to DHCP request packets.
DHCP snooping Support Bootp bind status	Indicates whether to enable DHCP Snooping to support BOOTP binding.
Interface	Interface name.
Trusted	Indicates whether an interface is a trusted port.
Rate limit	Rate limit for DHCP packets on an interface.

**Related Commands**

Command	Description
<b>ip dhcp snooping</b>	Enables the DHCP Snooping globally.
<b>ip dhcp snooping verify mac-address</b>	Enables the check of source MAC address of DHCP Snooping packets.
<b>ip dhcp snooping write-delay</b>	Sets the interval of writing user information to FLASH periodically.
<b>ip dhcp snooping information option</b>	Adds Option82 to the DHCP request message.
<b>ip dhcp snooping bootp-bind</b>	Enables the DHCP Snooping bootp bind function.
<b>ip dhcp snooping trust</b>	Sets the port as a trust port.

**Platform** N/A  
**Description**

### 1.19 show ip dhcp snooping binding

Use this command to display the information of the DHCP Snooping binding database.

**show ip dhcp snooping binding**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display all the information of the DHCP Snooping binding database.

**Configuration Examples** 1: The following example displays the information of the DHCP Snooping binding database.

```

Hostname# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS          IPADDRESS      LEASE (SEC)   TYPE          VLAN
INTERFACE
-----
-----
1      0000.0000.0001      1.1.1.1       78128         DHCP-Snooping 1
GigabitEthernet 0/1
2      0000.0000.0002      2.2.2.2       78111         DHCP-Snooping 1   WLAN 1
    
```

Parameter	Description
Total number of bindings	The total number of bindings in the DHCP Snooping database.
NO.	The record order.
MacAddress	The MAC address of the user.
IpAddress	The IP address of the user.
Lease(sec)	The lease time of the record.
Type	The record type.
VLAN	The VLAN where the user belongs.
INNER-VLAN	The inner VLAN of the user. It is applicable to all QINQ-termination products.
VXLAN	The VXLAN where the user belongs.
Interface	The user's connection interface. It can be a either a wired access interface or wireless access WLAN.

Related Commands	Command	Description
	<b>ip dhcp snooping binding</b>	Adds the static user information to the DHCP Snooping database.



**clear ip dhcp snooping binding**

Clears the dynamic user information from the DHCP Snooping binding database.

**Platform** N/A  
**Description**

# 1 DNS Commands

## 1.1 clear host

Use this command to clear the dynamically learned host name.

**clear host** [ \* | *host-name* ]

Parameter Description	Parameter	Description
	<i>host-name</i>	Deletes the specified dynamic domain name buffer.
	*	Deletes all dynamic domain name buffer.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** You can obtain the mapping record of the host name buffer table in two ways: 1) the **ip host** static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.

**Configuration Examples** The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.

```
Hostname#clear host *
```

Related Commands	Command	Description
	<b>show hosts</b>	Displays the host name buffer table.

**Platform** N/A

**Description**

## 1.2 ip domain-lookup

Use this command to enable DNS domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

**ip domain-lookup**

**no ip domain-lookup**

Restore the default configuration.

**default ip domain-lookup**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** -

**Configuration** The following example disables the DNS domain name resolution function.

**Examples**

```
Hostname(config)# no ip domain-lookup
```

Related Commands	Command	Description
	<b>show hosts</b>	Displays the DNS related configuration information.

**Platform Description** N/A

## 1.3 ip host

Use this command to configure a static mapping between a host name and an IP address.

**ip host** *host-name* [ *port-number* ] *ip-address*

Use this command to configure the mapping of the host name and the IP address. Use the **no** form of the command to remove the host list.

**ip host** *host-name* [ *port-number* ] *ip-address*

**no ip host** *host-name* [ *port-number* ] *ip-address*

Parameter Description	Parameter	Description
	<i>host-name</i>	The host name of the equipment
	<i>ip-address</i>	The IP address of the equipment

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures IPv4 address 192.168.5.243 for domain name www.test.com.

**Examples**

```
Hostname(config)# ip host www.test.com 192.168.5.243
```

**Related  
Commands**

Command	Description
<b>show hosts</b>	Show the DNS related configuration information.

**Platform** N/A

**Description**

## 1.4 ip name-server

Use this command to configure the IP address of the domain name server. Use the **no** form of this command to delete the configured domain name server.

**ip name-server** { *ip-address* | *ipv6-address* }

**no ip name-server** { *ip-address* | *ipv6-address* }

**Parameter  
Description**

Parameter	Description
<i>ip-address</i>	The IP address of the domain name server.
<i>ipv6-address</i>	The IPv6 address of the domain name server.

**Defaults** No domain name server is configured by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response.

Up to 6 DNS servers are supported. You can delete a DNS server with the *ip-address* option or all the DNS servers.

**Configuration** The following example configures the IPv4 domain name server and IPv6 domain name server.

**Examples**

```
Hostname(config)# ip name-server 192.168.5.134
Hostname(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800
2001:0DB8:0:f004::1
```

**Related  
Commands**

Command	Description
<b>show hosts</b>	Displays the DNS related configuration information.

**Platform** N/A

**Description**

## 1.5 ipv6 host

Use this command to configure a static mapping between a host name and an IPv6 address.

**ipv6 host** *host-name* [ *port-number* ] *ip-address*

Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the **no** form of the command to remove the host list.

**ipv6 host** *host-name* [ *port-number* ] *ipv6-address*

**no ipv6 host** *host-name* [ *port-number* ] *ipv6-address*

**Parameter Description**

Parameter	Description
<i>host-name</i>	The host name of the equipment
<i>port-number</i>	The port number for Telnet protocol
<i>ipv6-address</i>	The IPv6 address of the equipment

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide**

**Configuration** The following example configures the IPv6 address for the domain name.

**Examples**

```
Hostname(config)# ipv6 host switch 2001:0DB8:700:20:1::12
```

**Related Commands**

Command	Description
<b>show hosts</b>	Displays the DNS related configuration information.

**Platform** N/A

**Description**

## 1.6 show hosts

Use this command to display DNS configuration.

**show hosts** [ *hostname* ]

**Parameter**

Parameter	Description
-----------	-------------

<b>Description</b>	
	<i>hostname</i> Displays the specified domain name information,

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to display the DNS related configuration information.

**Configuration** Hostname# show hosts

**Examples** Name servers are:  
192.168.5.134 static

Host	type	Address	TTL(sec)
switch	static	192.168.5.243	---
www.test.com	dynamic	192.168.5.123	126

Field	Description
Name servers	Domain name server
Host	Domain name
type	Resolution type: Static resolution and dynamic resolution.
Address	IP address corresponding to the domain name
TTL	TTL of entries corresponding to the domain name/IP address.

<b>Related Commands</b>	Command	Description
	<b>ip host</b>	Configures the host name and IP address mapping by manual.
	<b>ipv6 host</b>	Configures the host name and IPv6 address mapping by manual.
	<b>ip name-server</b>	Configures the DNS server.

**Platform Description** N/A

# 1 DNS Snooping Commands

## 1.1 clear free-url

Use this command to clear authentication-free URLs.

**clear free-url**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged mode

**Usage Guide** Run this command to clear authentication-free URLs.

**Configuration Example** The following example clears authentication-free APP URLs.

```
Hostname# clear free-url
```

**Platform** N/A

## 1.2 free-url

Use this command to configure authentication-free URL.

**free-url { weixin | sina | iphone | url url }**

Use the **no** form of this command to clear authentication-free URL.

**no free-url { weixin | sina | iphone | url url }**

Parameter Description	Parameter	Description
	<b>weixin</b>	Indicates Weixin to be free of authentication.
	<b>sina</b>	Indicates Sina APPs to be free of authentication.
	<b>iphone</b>	Indicates specified iphone APP to be free of authentication.
	<i>url</i>	Indicates authentication-free URL.

**Defaults** By default, this function is disabled.

**Command Mode** Global configuration mode

14

**Usage Guide** You can configured multiple authentication-free URLs.

**Configuration** The following example configures authentication-free URL.

**Example**

```

Hostname# configure terminal
Hostname(config)# free-url weixin
    
```

**Verification** Run the **show free-url** command to check the authentication-free URL information.

**Common Errors** N/A

**Platform** N/A

### 1.3 ip dns snooping enable

Use this command to enable DNS snooping  
**ip dns snooping enable**

Use the no form of this command to disable DNS snooping  
**no ip dns snooping enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** DNS SNOOPING is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Run this command to enable DNS snooping.

**Configuration** The following example enables DNS snooping.

**Example**

```

Hostname#configure terminal
Hostname(config)#ip dns snooping enable
Hostname(config)#exit
    
```

**Verification** Run the **show run** command to display the configuration.

**Common** N/A



**Errors**

**Platform** It is supported only on switches.

## 1.4 show dns snooping statistics

Use this command to display DNS packet statistics.

**show dns snooping statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged mode, global configuration mode

**Usage Guide** Run this command to display statistics of DNS packets.

**Configuration Example** The following example displays DNS packet statistics.

```

Hostname# show dns snooping statistics
Receive dns request packet counts : 0
Receive dns reply packet counts : 0
Hostname#
    
```

Parameters:

Parameter	Description
N/A	N/A

**Platform** N/A

## 1.5 show free-url

Displays authentication-free URLs.

**show free-url**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged mode, global configuration mode

**Usage Guide** Run this command to display authentication-free URLs.

**Configuration** The following example displays authentication-free APP URLs.

**Example**

```

Hostname# show free-url
Total number of domain name : 4
Total number of ip address : 11

===== free-url domain name table =====
Host                type      Interface          Vlan      Wlan
*.qpic.cn           weixin   all                all       all
*.weixin.qq.com    weixin   all                all       all
weixin.qq.com       weixin   all                all       all
*.baidu.com         url      all                all       1
=====

===== free-url ip table =====
Host                type      Address            TTL(sec)
*.weixin.qq.com    weixin   61.151.224.41     2118
                  weixin   140.207.135.125   2118
                  weixin   140.207.54.47     2118
*.qpic.cn          weixin   140.206.160.234   2118
                  weixin   183.61.49.180    151
                  weixin   101.226.129.204   554
                  weixin   14.17.52.136     16
weixin.qq.com      weixin   14.17.42.45       800
*.baidu.com        url      115.239.210.246   19
                  url      115.239.211.235   2286
                  url      115.239.210.14    284
=====
    
```

Parameters:

Parameter	Description
Host	Indicates a domain name.
type	Indicates a type.
Address	Indicates an IP address.
TTL	Indicates time to live.

**Platform** N/A

# 1 IPv6 Basics Commands

## 1.1 clear ipv6 neighbors

Use this command to clear the dynamic IPv6 neighbors.

**clear ipv6 neighbors** [ *interface-id* ]

Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command does not clear all the dynamic neighbors on authentication VLAN. Note that the static neighbors will not be cleared.

 On an Overlay network, remote entries synchronized by EVPN cannot be manually deleted.

**Configuration** The following example clears all the dynamic IPv6 neighbors.

**Examples**

```
Hostname# clear ipv6 neighbors
```

The following example clears all dynamic IPv6 neighbors learned on the interface, GigabitEthernet 0/1.

```
Hostname# clear ipv6 neighbors gigabitEthernet 0/1
```

Related Commands	Command	Description
	ipv6 neighbor	Configures the neighbor.
	show ipv6 neighbors	Displays the neighbor information.

**Platform** N/A

**Description**

## 1.2 ipv6 address

Use this command to configure an IPv6 address for a network interface. Use the **no** form of this command to restore the default setting.

**ipv6 address ipv6-address/prefix-length**

**ipv6 address** *ipv6-prefix/prefix-length eui-64*

**ipv6 address** *prefix-name sub-bits/prefix-length* [ **eui-64** ]  
**no ipv6 address**  
**no ipv6 address** *ipv6-address/prefix-length*  
**no ipv6 address** *ipv6-prefix/prefix-length eui-64*  
**no ipv6 address** *prefix-name sub-bits/prefix-length* [ **eui-64** ]

Parameter	Parameter	Description
<b>Description</b>	<i>ipv6-prefix</i>	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>ipv6-address</i>	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>prefix-length</i>	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
	<i>prefix-name</i>	The general prefix name. Use the specified general prefix to generate the interface address.
	<i>sub-bits</i>	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
	<i>eui-64</i>	The generated IPV6 address consists of the address prefix and the 64 bit interface ID

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface.

The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the **ipv6 general-prefix** command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the *DHCPv6 Configuration*). Use the *sub-bits/prefix-length* parameter of this command to configure the sub-prefix and the host bit.

If no deleted address is specified when using **no ipv6 address**, all the manually configured addresses will be deleted.

**no ipv6 address** *ipv6-prefix/prefix-length eui-64* can be used to delete the addresses configured with **ipv6 address** *ipv6-prefix/prefix-length eui-64*.

**Configuration Examples** The following example configures an IPv6 address for the interface, BVI 1.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 address 2001:1::1/64

```

```

Hostname(config-if-BVI 1)# no ipv6 address 2001:1::1/64
Hostname(config-if-BVI 1)# ipv6 address 2002:1::1/64 eui-64
Hostname(config-if-BVI 1)# no ipv6 address 2002:1::1/64 eui-64
    
```

The following example configures an IPv6 address for the interface, GigabitEthernet 0/1, by using the general prefix.

```

Hostname(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix
0:0:0:7272::72/64
    
```

If *my-prefix* is set as 2001:1111:2222::/48, then the IPv6 address generated for an interface is 2001:1111:2222:7272::72/64.

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A  
**Description**

### 1.3 ipv6 address autoconfig

Use this command to automatically configure an IPv6 stateless address for a network interface. Use the **no** form of this command to restore the default setting.

```

ipv6 address autoconfig [ default ]
no ipv6 address autoconfig
    
```

Parameter	Parameter	Description
Description	<b>default</b>	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the <b>default</b> keyword

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address.

If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc.

**Configuration Examples** The following example automatically configures an IPv6 stateless address for a network interface.

```

Hostname(config-if-BVI 1)# ipv6 address autoconfig default
    
```

The following example restores the default setting.

```
Hostname(config-if-BVI 1)# no ipv6 address autoconfig
```

Related Commands	Command	Description
	<b>ipv6 address</b> <i>ipv6-prefix/prefix-length</i> [ <i>eui-64</i> ]	Configures the IPv6 address for the interface manually.

**Platform** N/A

**Description**

## 1.4 ipv6 icmp error-interval

Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval too-big** *milliseconds* [ *bucket-size* ]

Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the **no** form of this command to restore the default setting.

**ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

**no ipv6 icmp error-interval** *milliseconds* [ *bucket-size* ]

Parameter Description	Parameter	Description
	<i>milliseconds</i>	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
	<i>bucket-size</i>	Sets the number of tokens in the token bucket, in the range from 1 to 200.

**Defaults** The default *milliseconds* is 100 and *bucket-size* is 10.

**Command Mode** Global configuration mode

**Usage Guide** The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack,

If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and device sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6 error packet.

For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it

is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.

**Configuration Examples** The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second.

```
Hostname(config)# ipv6 icmp error-interval too-big 1000 100
```

The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second.

```
Hostname(config)# ipv6 icmp error-interval 1000 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.5 ipv6 enable

Use this command to enable the IPv6 function on an interface. Use the **no** form of this command to restore the default setting.

**ipv6 enable**

**no ipv6 enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** The IPv6 function of an interface can be enabled by configuring **ipv6 enable** or by configuring IPv6 address for the interface.

If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with **no ipv6 enable**.

**Configuration Examples** The following example enables IPv6 function on the interface BVI1.

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 enable
```

Related Commands	Command	Description
	show ipv6 interface	Displays the related information of an interface.

**Platform** N/A

**Description**

## 1.6 ipv6 general-prefix

Use this command to configure the IPv6 general prefix in the global configuration mode.

**ipv6 general-prefix** *prefix-name ipv6-prefix/prefix-length*

**no ipv6 general-prefix** *prefix-name ipv6-prefix/prefix-length*

Parameter	Parameter	Description
<b>Description</b>	<i>prefix-name</i>	The general prefix name.
	<i>pv6-prefix</i>	The network prefix value of the general-prefix following the format defined in RFC4291.
	<i>prefix-length</i>	The length of the general prefix.

**Defaults** N/A

**Command Mode** Global configuration mode.

**Usage Guide** It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix.

A general prefix could contain multiple prefixes.

These longer specified prefixes are usually used for the Ipv6 address configuration on the interface.

**Configuration** The following example configures manually a general prefix as my-prefix.

**Examples**

```
Hostname(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

Related	Command	Description
<b>Commands</b>	<b>ipv6 address prefix-name sub-bits/prefix-length</b>	Configures the interface address using the general prefix.
	<b>show ipv6 general-prefix</b>	Displays the general prefix.

**Platform** N/A

**Description**

## 1.7 ipv6 hop-limit

Use this command to configure the default hopcount to send unicast messages in the global configuration mode.

**ipv6 hop-limit** *value*

**no ipv6 hop-limit**



Parameter	Parameter	Description
<b>Description</b>	<i>value</i>	Hopcount ranging from 1 to 255.
<b>Defaults</b>	The default is 64.	
<b>Command Mode</b>	Global configuration mode.	
<b>Usage Guide</b>	This command takes effect for the unicast messages only, not for multicast messages.	
<b>Configuration Examples</b>	The following example sets the hopcount to 100.	
<b>Examples</b>	<pre>Hostname(config)# ipv6 hop-limit 100</pre>	
Related Commands	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.8 ipv6 mtu

Use this command to configure the MTU of IPv6 packets. Use the **no** form of this command to restore the default setting.

**ipv6 mtu** *bytes*  
**no ipv6 mtu**

Parameter	Parameter	Description
<b>Description</b>	<i>bytes</i>	MTU of IPv6 packets, in bytes. The value ranges from 1280 to 1500.
<b>Defaults</b>	The default configuration is the same as the configuration of the <b>mtu</b> command.	
<b>Command Mode</b>	Interface configuration mode	
<b>Usage Guide</b>	If the size of an IPv6 packet exceeds the IPv6 MTU, the RGOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.	
<b>Configuration Examples</b>	The following example sets the IPv6 MTU of the BVI 1 interface to 1400 bytes.	
<b>Examples</b>	<pre>Hostname(config)# interface bvi 1 Hostname(config-if-BVI 1)# ipv6 mtu 1400</pre>	

Related Commands	Command	Description
	<code>mtu</code>	Sets the MTU of an interface.

**Platform Description**

## 1.9 ipv6 nd cache interface-limit

Use this command to set the maximum number of neighbors learned on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd cache interface-limit** *value*

**no ipv6 nd cache interface-limit**

Parameter Description	Parameter	Description
	<i>value</i>	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to 2048. 0 indicates the number is not limited.

**Defaults** The default is 0.

**Command Mode** Interface configuration mode

**Usage Guide** This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. *limit* must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.

**Configuration Examples** The following example sets the number of neighbors learned on the interface to 100.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd cache interface-limit 100

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.10 ipv6 nd dad attempts

Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the **no** form of this command to restore it to the default setting.

**ipv6 nd dad attempts** *value*

**no ipv6 nd dad attempts** *value*

Parameter	Parameter	Description
Description	<i>value</i>	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.

**Defaults** The default is 1.

**Command Mode** Interface configuration mode.

**Usage Guide** When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the "tentative" status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the **down/up** interface. Whenever the state of an interface changes from **down** to **up**, the address collision check function of the interface will be enabled.

**Configuration Examples** The following example continuously sends 3 NS packets for IPv6 address collision check on the interface, BVI 1.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd dad attempts 3

```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A

**Description**

## 1.11 ipv6 nd dad retry

Use this command to set the interval for address conflict detection. Use the **no** form of this command to restore the default setting.

**ipv6 nd dad retry** *value*

**no ipv6 nd dad retry**

Parameter	Parameter	Description
Description	<i>value</i>	Sets the interval for address conflict detection, 60 seconds by default. Setting <i>value</i> to 0 indicates that the function is disabled.

**Defaults** The default value is 1.

**Command Mode** Global configuration mode

**Usage Guide** Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.

**Configuration** The following example sets the interval for address conflict detection to 10s.

**Examples**

```
Hostname(config)# ipv6 nd dad retry 10
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.12 ipv6 nd managed-config-flag

Use this command to set the “managed address configuration” flag bit of the RA message. Use the **no** form of this command to restore the default setting.

**ipv6 nd managed-config-flag**

**no ipv6 nd managed-config-flag**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command**

**Mode** Interface configuration mode.

**Usage Guide** This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.

**Configuration** The following example sets the “managed address configuration” flag bit of the RA message.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd managed-config-flag
```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd other-config-flag</b>	Sets the flag for obtaining all information except IP address through stateful auto configuration.

**Platform** N/A

**Description**

## 1.13 ipv6 nd max-opt

Use this command to set the ND option limit. Use the **no** form of this command to restore the default settings.

**ipv6 nd max-opt** *value*

**no ipv6 nd max-opt**

Parameter	Parameter	Description
<b>Description</b>	<i>value</i>	Sets the ND option limit, in the range from 1 to 100.

**Defaults** The default value is 10.

**Command mode** Global configuration mode.

**Usage Guide** The ND options include source link layer address option, MTU option, redirection option and prefix option.

**Configuration** The following example sets ND option limit to 20.

**Examples**

```
Hostname(config)# ipv6 nd max-opt 20
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.14 ipv6 nd ns-interval

Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation).

Use the **no** form of this command to restore the default setting.

**ipv6 nd ns-interval** *milliseconds*

**no ipv6 nd ns-interval**

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Interval for retransmitting NS in the range of 1,000 to 429,4967,295 milliseconds

**Defaults** The NS packet retransmission interval can be configured globally and on an L3 interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the NS packet retransmission interval is set to 3,000 ms in global configuration mode and set to 1,800 ms on SVI 1, the NS packet retransmission interval of SVI 1 is 1,800 ms. The NS packet retransmission interval of other interfaces (including newly created interfaces) is subject to the global configuration, that is, 3,000 ms.

**Command mode** Interface configuration mode, Global configuration mode.

**Usage Guide** The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.

**Configuration Examples** The following example sets the interval for the interface to retransmitting NS to 2 seconds.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd ns-interval 2000

```

The following example sets the NS packet retransmission interval to 3,000 ms in global configuration mode.

```

Hostname(config)# ipv6 nd ns-interval 3000

```

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.

**Platform Description** N/A

## 1.15 ipv6 nd other-config-flag

Use this command to set “other stateful configuration” flag bit of the RA message. Use the **no** form of this command to delete the flag bit.

**ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The flag bit is not set by default.

**Command**      Interface configuration mode.  
**mode**

**Usage Guide**      With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the **managed address configuration** is set, the default **other stateful configuration** is also set

**Configuration**      The following example sets “other stateful configuration” flag bit of the RA message.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd other-config-flag

```

Related	Command	Description
Commands	show ipv6 interface	Displays the interface information.

**Platform**      N/A  
**Description**

## 1.16 ipv6 nd prefix

Use this command to configure the address prefix included in the RA. Use the **no** form of this command to delete the set prefix or restore the default setting.

```

ipv6 nd prefix { ipv6-prefix/prefix-length | default } [ [ valid-lifetime { infinite | preferred-lifetime } ] |
[ at valid-date preferred-date ] | [ infinite { infinite | preferred-lifetime } ] ] [ no-advertise ] |
[ [ off-link ] [ no-autoconfig ] ] [ pool pool-name ] | [ preference { high | medium | low } ] [ proxy ] ]
no ipv6 nd prefix { ipv6-prefix | prefix-length | default }

```

Parameter	Parameter	Description
<b>Description</b>	<i>ipv6-prefix</i>	IPv6 network ID following the format defined in RFC4291
	<i>prefix-length</i>	Length of the IPv6 prefix. “/” shall be added in front of the prefix
	<i>valid-lifetime</i>	Valid lifetime of the RA prefix received by the host
	<i>preferred-lifetime</i>	Preferred lifetime of the RA prefix received by the host
	<i>at valid-date preferred-date</i>	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
	<b>infinite</b>	Indicates that the prefix is always valid.
	<b>default</b>	Sets the default prefix.
	<b>no-advertise</b>	The prefix will not be advertised by the device.
	<b>off-link</b>	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
	<b>no-autoconfig</b>	Indicates that the RA prefix received by the host cannot be used for auto address configuration.

<b>pool</b> <i>pool-name</i>	Configures a specific prefix pool to be bound to an interface to ensure that different IPv6 prefixes are allocated to different users.
<b>preference</b>	Sets the routing priority. The value is <b>high</b> , <b>medium</b> , or <b>low</b> . The default value is <b>medium</b> .
<b>proxy</b>	Enables the ND proxy based on the prefix.

**Defaults** By default, the advertised prefix is the one set with **ipv6 address** on the interface. The default parameters of the prefix configured in the RA are as follows:

*valid-lifetime*: 2592000s (30 days)

*preferred-lifetime*: 604800s (7 days)

**preference**: medium

**proxy**: disabled

The prefix is advertised and is used for on-link judgment and auto address configuration.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with **ipv6 address** on the interface. To add other prefixes, use this command.

**ipv6 nd prefix default**

Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with **ipv6 nd prefix default** will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with **ipv6 nd prefix default**; only the prefix that uses all the default configurations can be modified with this command.

**at** *valid-date preferred-date*

The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).

**Configuration** The following example adds a prefix for BVI 1.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd prefix 2001::/64 infinite 2592000

```

The following example sets the default prefix parameters for BVI 1 (they cannot be used for auto address configuration):

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 prefix default no-autoconfig

```

If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.

**Related  
Commands**

Command	Description
<b>show ipv6 interface</b>	Displays the RA information of an interface.



**Platform** N/A  
**Description**

## 1.17 ipv6 nd ra-hoplimit

Use this command to set the hopcount of the RA message. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-hoplimit** *value*  
**no ipv6 nd ra-hoplimit**

Parameter	Parameter	Description
Description	<i>value</i>	Hopcount

**Defaults** The default is 64.

**Command Mode** Interface configuration mode.

### Usage Guide

**Configuration Examples** The following example sets the hopcount of the RA message to 110 on the interface, BVI 1.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd ra-hoplimit 110

```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA message.
	<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA message.

**Platform** N/A  
**Description**

## 1.18 ipv6 nd ra-interval

Use this command to set the interval of sending the RA. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-interval** { *seconds* | **min-max** *min\_value* *max\_value* }  
**no ipv6 nd ra-interval**

Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending the RA message in seconds, 3-1800s.

<b>min-max</b>	Maximum and minimum interval sending the RA message in seconds
<i>min_value</i>	Minimum interval sending the RA message in seconds
<i>max_value</i>	Maximum interval sending the RA message in seconds

**Defaults** 200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value.

If the key word **min-max** is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.

**Configuration** The following example sets the interval of sending the RA to 110 seconds.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd ra-interval 110

```

The following example sets the interval of sending the RA from 110 to 120 seconds.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd ra-interval min-max 110 120

```

Related	Command	Description
<b>Commands</b>	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
	<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA message.
	<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA message.

**Platform** N/A

**Description**

## 1.19 ipv6 nd ra-lifetime

Use this command to set the device lifetime of the RA sent on the interface. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-lifetime** *seconds*

**no ipv6 nd ra-lifetime**

Parameter	Parameter	Description
<b>Description</b>	<i>seconds</i>	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.

**Defaults** The default is 1800.

**Command Mode** Interface configuration mode.

**Usage Guide** The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)

**Configuration Examples** The following example sets the device lifetime of the RA sent on the interface to 2,000 seconds.

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd ra-lifetime 2000

```

Related Commands	Command	Description
	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA.
	<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA.
	<b>ipv6 nd ra-mtu</b>	Sets the MTU of the RA.

**Platform Description** N/A

## 1.20 ipv6 nd ra-mtu

Use this command to set the MTU of the RA message. Use the **no** form of this command to restore the default setting.

**ipv6 nd ra-mtu** *value*  
**no ipv6 nd ra-mtu**

Parameter	Parameter	Description
<b>Description</b>	<i>value</i>	MTU value, in the range from 0 to 4294967295.

**Defaults** IPv6 MTU value of the network interface.

**Command Mode** Interface configuration mode.

**Usage Guide** If it is specified as 0, the RA will not have the MTU option

**Configuration Examples** The following example sets the MTU of the RA message to 1,400 bytes.

```

Hostname(config)# interface bvi 1

```

```
Hostname(config-if-BVI 1)# ipv6 nd ra-mtu 1400
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.
	<b>ipv6 nd ra-lifetime</b>	Sets the lifetime of the device.
	<b>ipv6 nd ra-interval</b>	Sets the interval of sending the RA message.
	<b>ipv6 nd ra-hoplimit</b>	Sets the hopcount of the RA message.

**Platform** N/A

**Description**

## 1.21 ipv6 nd reachable-time

Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the **no** form of this command to restore the default setting.

**ipv6 nd reachable-time** *milliseconds*

**no ipv6 nd reachable-time**

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Reachable time for the neighbor in the range from 0 to 3,600,000 in the unit of milliseconds.

**Defaults** The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30000 milliseconds (30 seconds) when the device discovers the neighbor.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time.

The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.

According to RFC4861, the actual time to reach neighbor is not consistent with the configured value, ranging from 0.5\*configured value to 1.5\*configured value.

**Configuration** The following example sets the reachable time to 1,000 seconds.

**Examples**

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd reachable-time 1000000
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A

**Description**

## 1.22 ipv6 nd stale-time

Use this command to set the period for the neighbor to maintain the state. Use the **no** form of this command to restore the default setting.

**ipv6 nd stale-time** *seconds*

**no ipv6 nd stale-time**

Parameter	Parameter	Description
<b>Description</b>	<i>seconds</i>	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.

**Defaults** The default is 3600.

**Command** Global configuration mode, Interface configuration mod

**Mode**

**Usage Guide** This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.

This command can be configured on an interface or in global configuration mode. The configuration configured on an interface takes priority over that configured in global configuration mode. That is, if the duration is configured on an interface, the duration configured on the interface applies. Otherwise, the global configuration will apply.

**Configuration** The following example sets the period to 600 seconds for the neighbor to maintain the state.

**Examples**

```
Hostname(config)# ipv6 nd stale-time 600
```

The following example sets the duration in which a neighbor keeps in stale state to 600s on SVI 1.

```
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ipv6 nd stale-time 600
```

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A

**Description**

## 1.23 ipv6 nd suppress-auth-vlan-ns

Run this command to configure an interface not to send NS packets to an authenticated VLAN.

**ipv6 nd suppress-auth-vlan-ns**

Run this command to remove this configuration.

**no ipv6 nd suppress-auth-vlan-ns**

Parameter Description	Parameter	Description
	N/A	N/A
<b>Defaults</b>	Interfaces in an IPv6-enabled super VLAN will not send NS packets to an authenticated sub VLANs by default.	
<b>Command Mode</b>	Interface configuration mode	
<b>Default Level</b>	14	
<b>Usage Guide</b>	The command is supported only on SVIs and takes effect in gateway authentication mode.	
<b>Configuration Examples</b>	The following example configures SVI 2 to send NS packets to an authenticated VLAN.	
<b>Examples</b>	<pre> Hostname(config)# interface vlan 2 Hostname(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns </pre>	
<b>Verification</b>	Run the <b>show running-config Interface</b> command to show the configuration.	
<b>Notifications</b>	N/A	
<b>Common Errors</b>	N/A	
<b>Platform Description</b>	N/A	

## 1.24 ipv6 nd suppress-ra

Use this command to disable the interface from sending the RA message. Use the **no** form of this command to enable the function.

**ipv6 nd suppress-ra**

**no ipv6 nd suppress-ra**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ipv6 nd suppress-ra** command is enabled by default.

**Command Mode** Interface configuration mode.

#### Usage Guide

**Configuration** The following example disables the interface from sending the RA message.

#### Examples

```
Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 nd suppress-ra
```

Related	Command	Description
Commands	<b>show ipv6 interface</b>	Displays the interface information.

**Platform** N/A  
**Description**

## 1.25 ipv6 nd unresolved

Use this command to set the maximum number of the unresolved neighbor table entries. Use the **no** form of this command to restore the default setting.

**ipv6 nd unresolved** *number*  
**no ipv6 nd unresolved**

Parameter	Parameter	Description
Description	<i>number</i>	Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to 2048.

**Defaults** The default is 0. (The maximum number is the neighbor table size supported by the device)

**Command Mode** Global configuration mode

**Usage Guide** This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources,

**Configuration** The following example sets the maximum number of the unresolved neighbor table entries to 200.

#### Examples

```
Hostname(config)# ipv6 nd unresolved 200
```

Related	Command	Description
---------	---------	-------------

<b>Commands</b>	N/A	N/A
-----------------	-----	-----

**Platform** N/A

**Description**

## 1.26 ipv6 neighbor

Use this command to configure a static neighbor. Use the **no** form of this command to delete a static neighbor.

**ipv6 neighbor** *ipv6-address interface-id hardware-address*

**no ipv6 neighbor** *ipv6-address interface-id*

Parameter	Parameter	Description
<b>Description</b>	<i>ipv6-address</i>	The neighbor IPv6 address, in the form as defined in RFC4291.
	<i>interface-id</i>	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
	<i>hardware-address</i>	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.

**Defaults** No static neighbor is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command.

If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the `show ipv6 neighbor static` command to display the state of the static neighbor.

Use the **clear ipv6 neighbors** command to clear all neighbors learned dynamically through NDP.

**Configuration** The following example configures a static neighbor on SVI 1.

**Examples**

```
Hostname(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform** N/A



**Description**

## 1.27 ipv6 ns-linklocal-src

Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the **no** form of this command to use the global IP address as the source address to send neighbor requests.

**ipv6 ns-linklocal-src**

**no ipv6 ns-linklocal-src**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The local address of the link is always used as the source address to send neighbor requests.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures not to use the link-local address as the source address for sending NS packets:

```

Hostname# configure terminal
Hostname(config)# ipv6 ns-linklocal-src

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.28 ipv6 redirects

Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the **no** form of this command to restore the default setting.

**ipv6 redirects**

**no ipv6 redirects**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is enabled by default.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** -

**Configuration** The following example enables ICMPv6 redirection on interface BVI1.

**Examples**

```

Hostname(config)# interface bvi 1
Hostname(config-if-BVI 1)# ipv6 redirects

```

Related	Command	Description
Commands	show ipv6 interface	Displays the interface information.

**Platform** N/A

**Description**

## 1.29 ipv6 source-route

Use this command to forward the IPv6 packet with route header. Use the **no** form of this command to restore the default setting.

**ipv6 source-route**

**no ipv6 source-route**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The **ipv6 source-route** command is disabled by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.

**Configuration** The following example forwards the IPv6 packet with route header.

**Examples**

```

Hostname(config)# no ipv6 source-route

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.30 show ipv6 address

Use this command to display the IPv6 addresses.

**show ipv6 address** [ *interface-name* ]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays all IPv6 address configured on the device.

**Examples**

```

Hostname# show ipv6 address
Global unicast address limit: 16, Global unicast address count: 2
Tentative address count: 0,Duplicate address count: 0
Preferred address count: 4,Deprecated address count: 0
  dialer 1
    1:1:1:1::F/64                               Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    FE80::5A69:6CFF:FE1A:CE13/64                Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
  dialer 2
    FE80::5A69:6CFF:FE1A:CE13/64                Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    2:2:2:2::F/64                               Preferred
    Preferred lifetime: INFINITE, Valid lifetime: INFINITE

```

The following example displays the IPv6 address configured on the BVI 1.

```

Hostname# show ipv6 address bvi 1
Global unicast address count: 2
Tentative address count: 0,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0

```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.31 show ipv6 general-prefix

Use this command to display the information of the general prefix.

**show ipv6 general-prefix**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command** Privileged EXEC mode.

**Mode**

**Usage Guide** Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.

**Configuration** The following example displays the information of the general prefix.

**Examples**

```

Hostname# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual configuration
 2001:1111:2222::/48
 2001:1111:3333::/48

```

Related	Command	Description
Commands	<b>ipv6 general-prefix</b>	Configures the general prefix.

**Platform** N/A

**Description**

## 1.32 show ipv6 interface

Use this command to display the IPv6 interface information.

**show ipv6 interface** [ [ *interface-id* ] [ **ra-info** ] ] [ *brief* [ *interface-id* ] ]

Parameter	Parameter	Description
Description	<i>interface-id</i>	Interface (including Ethernet interface, aggregate port, or SVI)
	<b>ra-info</b>	Displays the RA information of the interface.
	<i>brief</i>	Displays the brief information of the interface (interface status and address information).

**Defaults** N/A

**Command Mode**

**Usage Guide** Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.

**Configuration** The following example displays the information of the IPv6 interface.

**Examples**

```

Hostname# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds

```

The following line is included in the above information: 2001::1, subnet is 2001::/64 **[TENTATIVE]**.

The flag bit in the [ ] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.

DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.
PRE	Indicates the address automatically generated.
GEN	Indicates the address using the general prefix.

The following example displays the RA information of the IPv6 interface.

```

Hostname# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/1, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)

```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.

!M   M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O   O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

Field	Meaning
total	The number of the prefixes of the interface.
fec0:1:1:1::/64	A specific prefix.
Def	Indicate that the interfaces use the default prefix.
Auto   CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
!Adv	Indicate that the prefix will not be advertised.
vlttime	Valid lifetime of the prefix, measured in seconds.
pltime	Preferred lifetime of the prefix, measured in seconds.
L   !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
A   !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.

The following example displays the brief information of the IPv6 interface.

```
Hostname#show ipv6 interface brief
```

```
GigabitEthernet 0/1          [down/down]
    2222::2
    FE80::1614:4BFF:FE5C:ED3A
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

### 1.33 show ipv6 neighbors

Use this command to display the IPv6 neighbors.

```
show ipv6 neighbors [ verbose ] [ interface-id ] [ ipv6-address ] [static] [ oob ]
```

Parameter Description	Parameter	Description
	<b>verbose</b>	Displays the neighbor details.
	<i>interface-id</i>	Displays the neighbors of the specified interface.

<i>ipv6-address</i>	Displays the neighbors of the specified IPv6 address.
<b>static</b>	Displays the validity status of static neighbors.
<b>oob</b>	Displays IPv6 neighbors learned on the MGMT interface.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide**

**Configuration** Show the neighbor details:

**Examples**

```

Hostname# show ipv6 neighbors verbose
IPv6 Address Linklayer Addr Interface
2001::1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1
  State: Reach/H Age: - asked: 0
    
```

Field	Meaning
IPv6 Address	IPv6 address of the Neighbor
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.
Interface	Interface the neighbor locates.
State	<p>State of the neighbor: state/H(R)</p> <p>The values of STATE are as below:</p> <p>INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received.</p> <p>REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor.</p> <p>STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor.</p> <p>DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD.</p> <p>PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3).</p>



	? : Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.
Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.
Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.

The following example displays status of static neighbors.

```

Hostname# show ipv6 neighbors static
IPv6 Address      Linklayer Addr  Interface          State
2001:1::1         00d0.f822.33ab  GigabitEthernet 0/14  ACTIVE
2001:2::2         00d0.f822.33ac  VLAN 1             INACTIVE
    
```

Field	Meaning
IPv6 Address	IPv6 addresses of the static neighbors
Linklayer Addr	Link addresses, namely, MAC addresses.
Interface	Interfaces the neighbors locate.
State	States of the static neighbors: The values of STATE are as below: ACTIVE INACTIVE

Related Commands	Command	Description
	<b>ipv6 neighbor</b>	Configures a neighbor.

Platform N/A

Description

### 1.34 show ipv6 neighbors statistics

Use the following commands to display the statistics of one IPv6 neighbors.

```
show ipv6 neighbors statistics [ all ]
```

Parameter Description	Parameter	Description
	<b>all</b>	Displays the statistics on all IPv6 neighbor tables.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays the statistics of the global neighbors.

**Examples**

```
Hostname#show ipv6 neighbor statistics
```

```
Memory: 0 bytes
```

```
Entries: 0
```

```
  Static: 0,Dynamic: 0,Local: 0
```

```
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
```

The following example displays the statistics of all neighbors.

```
Hostname#show ipv6 neighbor statistics all
```

```
IPv6 neighbor table count: 1
```

```
Static neighbor count: 0(0 active, 0 inactive)
```

```
Total
```

```
Memory: 0 bytes
```

```
Entries: 0
```

```
  Static: 0,Dynamic: 0,Local: 0
```

```
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
```

```
Global
```

```
Memory: 0 bytes
```

```
Entries: 0
```

```
  Static: 0,Dynamic: 0,Local: 0
```

```
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

## 1.35 show ipv6 neighbor statistics per-mac

Use this command to display the number of neighbor entries of every MAC address.

**show ipv6 neighbor statistics per-mac** [*interface-name*] [*mac-address*]

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface ID
	<i>mac-address</i>	MAC address

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the number of neighbor entries of every MAC address.

```

Hostname# show ipv6 neighbor statistics per-mac
Interface  MAC address      Statistics
-----
VLAN 1    0000:0000:0001      3
VLAN 1    0000:0000:0002      5
VLAN 2    0000:0000:0003     10

```

Field	Description
Interface	Interface ID.
MAC address	MAC address.
Statistics	ND entry number.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.36 show ipv6 packet statistics

Use this command to display the statistics of IPv6 packets.

**show ipv6 packet statistics** [ **total** | *interface-name* ]

Parameter	Parameter	Description
Description	<b>total</b>	Displays total statistics of all interfaces.
	<i>interface-name</i>	Interface name

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the total statistics of the Ipv6 packets and the statistics of each interface.

```

Hostname# show ipv6 packet statistics
Total
  Received 54006 packets, 5396241 bytes
    Unicast:1958,Multicast:52048
  Discards:11106
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:11106
  Sent 4683 packets, 406688 bytes
    Unicast:4678,Multicast:5
AP680CD-JP#show ipv6 packet statistics
Total
  Received 54022 packets, 5397633 bytes
    Unicast:1958,Multicast:52064
  Discards:11106
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:11106
  Sent 4715 packets, 409472 bytes
    Unicast:4710,Multicast:5
    
```

The following example displays the total statistics of the Ipv6 packets.

```

Hostname# show ipv6 packet statistics total
Total
  Received 54034 packets, 5398681 bytes
    Unicast:1958,Multicast:52076
  Discards:11106
    HdrErrors:0 (HoplimitExceeded:0,Others:0)
    NoRoutes:0
    Others:11106
  Sent 4739 packets, 411568 bytes
    Unicast:4734,Multicast:5
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description**

## 1.37 show ipv6 raw-socket

Use this command to display all IPv6 raw sockets.

**show ipv6 raw-socket** [ *num* ]

Parameter	Parameter	Description
Description	<u>num</u>	Protocol.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays all IPv6 raw sockets.

### Examples

```
Hostname# show ipv6 raw-socket
```

```
Number Protocol Process name
```

```
1 ICMPv6 vrrp.elf
```

```
2 ICMPv6 tcpip.elf
```

```
3 VRRP vrrp.elf
```

```
Total: 3
```

Field	Description
Number	Number.
Protocol	Protocol.
Process name	Process number.
Total	Total number of IPv6 raw sockets.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.38 show ipv6 routers

On the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.

**show ipv6 routers** [ *interface-type interface-number* ]

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	<i>interface-type</i> <i>interface-number</i>	(Optional) Displays the routing advertisement of the specified interface.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode.	
<b>Usage Guide</b>	Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.	

**Configuration** The following example displays the IPv6 router

**Examples**

```

Hostname# show ipv6 routers
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
  Preference=MEDIUM
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 6001:3::/64 onlink autoconfig
  Valid lifetime 2592000 sec, preferred lifetime 604800 sec
  Prefix 6001:2::/64 onlink autoconfig
  Valid lifetime 2592000 seconds, preferred lifetime 604800 seconds

```

Related	Command	Description
<b>Commands</b>	N/A	N/A

**Platform Description** N/A

## 1.39 show ipv6 sockets

Use this command to display all IPv6 sockets.

**show ipv6 sockets**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays all IPv6 sockets.

**Examples**

```

Hostname# show ipv6 sockets
Number Process name      Type   Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf      RAW   ICMPv6   :::58         :::0            *
2      tcpip.elf     RAW   ICMPv6   :::58         :::0            *
3      vrrp.elf      RAW   VRRP     :::112        :::0            *
4      rg-snmpd     DGRAM UDP      :::161        :::0            *
5      rg-snmpd     DGRAM UDP      :::162        :::0            *
6      dhcp6.elf    DGRAM UDP      :::547        :::0            *
7      rg-sshd      STREAM TCP     :::22         :::0            LISTEN
8      rg-telnetd   STREAM TCP     :::23         :::0            LISTEN
Total: 8
    
```

Field	Description
Number	Number.
Process name	Process name.
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.
Protocol	Protocol number
LocalIP:Port	Local IPv6 address and port.
ForeignIP:Port	Peer IPv6 address and port.
State	State (for IPv6 TCP sockets).
Total	Total number of sockets.

**Related**

Command	Description
N/A	N/A

**Commands**

**Platform** N/A

**Description**

## 1.40 show ipv6 udp

Use this command to display all IPv6 UDP sockets.

**show ipv6 udp [ local-port num ] [ peer-port num ]**

Use this command to display IPv6 UDP socket statistics.

**show ipv6 udp statistics**

**Parameter**

Parameter	Description
<b>local-port num</b>	Local port number.
<b>peer-port num</b>	Peer port number.

**Description**

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays all IPv6 UDP sockets.

**Examples**

```

Hostname# show ipv6 udp
Number Local Address Peer Address Process name
1      :::161          :::0          rg-snmpd
2      :::162          :::0          rg-snmpd
3      :::547          :::0          dhcp6.elf
    
```

Filed	Description
Number	Number.
Local Address	Local IPv6 address and port.
Peer Address	Peer IPv6 address and port.
Process name	Process name.

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**



# 1 DHCPv6 Commands

## 1.1 clear ipv6 dhcp binding

Use this command to clear the DHCPv6 binding information.

**clear ipv6 dhcp binding** [ *ipv6-address* ]

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<i>ipv6-address</i>	Sets the IPv6 address or the prefix.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	If the <i>ipv6-address</i> is not specified, all DHCPv6 binding information is cleared. If the <i>ipv6-address</i> is specified, the binding information for the specified address is cleared.	
<b>Configuration Examples</b>	The following example clears the DHCPv6 binding information:	
	<pre>Hostname# clear ipv6 dhcp binding</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.2 clear ipv6 dhcp client

Use this command to reset the DHCPv6 client.

**clear ipv6 dhcp client***interface-type interface-number*

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<i>interface-type interface-number</i>	Sets the interface type and the interface number.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	

**Usage Guide** This command is used to reset the DHCPv6 client, which may lead the client to request for the configurations from the server again.

**Configuration** The following example resets DHCP client VLAN 1.

**Examples**

```
Hostname# clear ipv6 dhcp client vlan 1
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.3 clear ipv6 dhcp conflict

Use this command to clear the DHCPv6 address conflicts.

**clear ipv6 dhcp conflict** { *ipv6-address* | \* }

Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Specifies IPv6 address or prefix.
	*	All IPv6 addresses or prefixes

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the \* parameter is not specified, all conflicts of IPv6 addresses or prefixes will be deleted. If the *ipv6-address* parameter is specified, only the specified address conflict will be deleted.

**Configuration** The following example clears a DHCPv6 address conflict.

**Examples**

```
Hostname# clear ipv6 dhcp conflict 2008:50::2
```

Related Commands	Command	Description
	<b>show ipv6 dhcp conflict</b>	Displays address conflicts.

**Platform Description** N/A

### 1.4 clear ipv6 dhcp server statistics

Use this command to clear the DHCPv6 server statistics.

**clear ipv6 dhcp server statistics**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the DHCPv6 server statistics.	
Configuration	The following example clears the DHCPv6 server statistics.	
Examples	<pre>Hostname# clear ipv6 dhcp server statistics</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

## 1.5 dns-server

Use this command to set the DNS Server list information for the DHCPv6 Server.

Use the **no** form of this command to restore the default setting.

**dns-server** *ipv6-address*

**no dns-server** *ipv6-address*

Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the IPv6 address or the DNS server.
Defaults	By default, no DNS server list is configured.	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	To configure several DNS Server addresses, use the <b>dns-server</b> command for several times. The newly-configured DNS Server address will not overwrite the former ones.	
Configuration	The following example configures the DNS server address.	
Examples	<pre>Hostname(config)# ipv6 dhcp pool pool1 Hostname(config-dhcp)# dns-server 2008:1::1</pre>	

Related Commands	Command	Description
	<b>domain-name</b>	Sets the DHCPv6 domain name information.
	<b>ipv6 dhcp pool</b>	Sets a DHCPv6 pool.

**Platform** N/A  
**Description**

## 1.6 domain-name

Use this command to set the domain name for the DHCPv6 server.

Use the **no** form of this command to restore the default setting.

**domain-name** *domain*

**no domain-name** *domain*

Parameter Description	Parameter	Description
	<i>domain</i>	Sets the domain name.

**Defaults** By default, no domain name is configured.

**Command Mode** DHCPv6 pool configuration mode

**Usage Guide** To configure several domain names, use the domain-name command for several times. The newly-configured domain name will not overwrite the former ones.

**Configuration** The following example sets the domain name for the DHCPv6 server to example.com.

**Examples**

```
Hostname(config)# ipv6 dhcp pool mypool0
Hostname(config-dhcp)# domain-name example.com
```

Related Commands	Command	Description
	<b>dns-server</b>	Sets the DHCPv6 DNS server list.
	<b>ipv6 dhcp pool</b>	Sets the DHCPv6 pool.

**Platform** N/A  
**Description**

## 1.7 ipv6 dhcp client ia

Use this command to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server. Use the **no** form of this command to restore the default setting.

**ipv6 dhcp client ia** [**rapid-commit**]

**no ipv6 dhcp client ia**

Parameter	Parameter	Description
Description	<b>rapid-commit</b>	Allows the two-message interaction process.

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** This command is used to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server,  
The **rapid-commit**key allows the two-message interaction process between the client and the server. After the key is configured, the solicit message transmitted by the client contains the rapid-commit option.

**Configuration Examples** The following example enables the request for the IANA address on the interface.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client ia

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.8 ipv6 dhcp client pd

Use this command to enable the DHCPv6 client and request for the prefix address information.

Use the **no** form of this command to restore the default setting.

**ipv6 dhcp client pd** *prefix-name* [ **rapid-commit** ]

**no ipv6 dhcp client pd**

Parameter	Parameter	Description
Description	<i>prefix-name</i>	Defines the IPv6 prefix name.
	<b>rapid-commit</b>	Allows the two-message interaction process.

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode

**Usage Guide** With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface.

With the **ipv6 dhcp client pd** command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server

The keyword **rapid-commit** allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the **rapid-commit** item.

**Configuration** The following example enables the prefix information request on the interface.

**Examples**

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client pd pd_name
```

**Related  
Commands**

Command	Description
<b>clear ipv6 dhcp client</b>	Resets the DHCPv6 client function on the interface.
<b>show ipv6 dhcp interface</b>	Displays the DHCPv6 interface configuration.

**Platform** N/A

**Description**

## 1.9 ipv6 dhcp pool

Use this command to set the DHCPv6 server pool.

Use the **no** form of this command to restore the default setting.

**ipv6 dhcp pool** *poolname*

**no ipv6 dhcp pool** *poolname*

**Parameter  
Description**

Parameter	Description
<i>poolname</i>	Defines the DHCPv6 pool name.

**Defaults** By default, no DHCPv6 server pool is configured.

**Command  
Mode** Global configuration mode

**Usage Guide** This command is used to create a DHCPv6 Server configuration pool. After configuring this command, it enters the DHCPv6 pool configuration mode, in which the administrator can set the pool parameters, such as the prefix and the DNS Server information, ect.

After creating the DHCPv6 Server configuration pool, use the **ipv6 dhcp server** command to associate the pool and the DHCPv6 Server on one interface.

**Configuration** The following example sets the DHCPv6 server pool.

**Examples**

```
Hostname# configure terminal
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)#
```

Related Commands	Command	Description
	<b>ipv6 dhcp server</b>	Enables the DHCPv6 server function on the interface.
	<b>show ipv6 dhcp pool</b>	Displays the DHCPv6 pool information.

**Platform** N/A

**Description**

## 1.10 ipv6 dhcp server

Use this command to enable the DHCPv6 server on the interface.

Use the **no** form of this command to restore the default setting.

**ipv6 dhcp server** *poolname* [ **rapid-commit** ] [ **preference** *value* ]

**no ipv6 dhcp server**

Parameter	Parameter	Description
<b>Description</b>	<i>poolname</i>	Defines the DHCPv6 pool name.
	<b>rapid-commit</b>	Allows the two-message interaction process.
	<b>preference</b> <i>value</i>	Sets the preference level for the advertise message. The valid range is from 1 to 100 and the default value is 0.

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Mode**

**Usage Guide** Use the **ipv6 dhcp server** command to enable the DHCPv6 service.

Configuring the keyword **rapid-commit** allows the two-message interaction for the server and the client when allocating the address prefix and setting other configurations. With this keyword configured, if the client solicit message includes the **rapid-commit** item, the DHCPv6 Server will send the Reply message immediately.

DHCPv6 Server carries with the **preference** value when sending the advertise message if the **preference** level is not 0.

If the **preference** level is 0, the advertise message will not include this field. If the **preference** value is 255, the client sends the request message to the server to obtain the configurations.

DHCPv6 Client, Server and Relay functions are exclusive, and only one of the functions can be configured on the interface.

**Configuration** The following example enables the DHCPv6 server on the interface.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp server pool1

```

Command	Description
---------	-------------

<b>Related Commands</b>	<b>ipv6 dhcp pool</b>	Sets the DHCPv6 pool.
	<b>show ipv6 dhcp pool</b>	Displays the DHCPv6 pool information.

**Platform** N/A  
**Description**

## 1.11 ipv6 local pool

Use this command to configure the local prefix pool of the DHCPv6 server prefix.

Use the **no** form of this command to restore the default setting.

**ipv6 local pool** *poolname prefix/prefix-length assigned-length*

**no ipv6 local pool** *poolname*

Parameter	Parameter	Description
<b>Description</b>	<i>poolname</i>	The local prefix pool name
	<i>prefix/prefix-length</i>	The prefix and prefix length
	<i>assigned-length</i>	The assigned prefix length

**Defaults** By default, no local prefix pool of the DHCPv6 server prefix is configured.

**Command Mode** Global configuration mode

**Usage Guide** The **ipv6 local pool** command is used to create the local prefix pool. If the DHCPv6 server requires prefix delegation, you can use the **prefix-delegation pool** command to specify the local prefix pool and then assign prefixes from the prefix pool.

**Configuration** The following example configures the local prefix pool.

**Examples**

```
Hostname(config)# ipv6 local pool client-prefix-pool 2001::db8::/64 80
```

The following example specifies the local prefix pool.

```
Hostname(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime
2000 1000
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.12 prefix-delegation

Use this command to set the static binding address prefix information for the DHCPv6 server.

Use the **no** form of this command to restore the default setting.



**prefix-delegation** *ipv6-prefix/prefix-length client-DUID [ lifetime ]*  
**no prefix-delegation** *ipv6-prefix/prefix-length client-DUID [ lifetime ]*

Parameter	Parameter	Description
Description	<i>ipv6-prefix/prefix-length</i>	Sets the IPv6 address prefix and the prefix length.
	<i>client-DUID</i>	Sets the client DUID.
	<i>lifetime</i>	Sets the interval of using the prefix by the client.

**Defaults** By default, no address prefix information is configured.  
The default *lifetime* is 3600 seconds (one hour).

**Command Mode** DHCPv6 pool configuration mode

**Usage Guide** The administrator uses this command to manually set the address prefix information list for the client IA\_PD and set the valid lifetime for those prefixes.  
The parameter *client-DUID* allocates the address prefix to the first IA\_PD in the specified client.  
Before receiving the request message for the address prefix from the client, DHCPv6 Server searches for the corresponding static binding first. If it succeeds, the server returns to the static binding; otherwise, the server will attempt to allocate the address prefix from other prefix information sources.

**Configuration Examples** The following example sets the static binding address prefix information for the DHCPv6 server.

```
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac
```

Related Commands	Command	Description
	<b>ipv6 dhcp pool</b>	Sets a DHCPv6 pool.
	<b>ipv6 local pool</b>	Sets a local prefix pool.
	<b>prefix-delegation pool</b>	Specifies the DHCPv6 local prefix pool.
	<b>show ipv6 dhcp pool</b>	Displays the DHCPv6 pool information.

**Platform** N/A  
**Description**

## 1.13 prefix-delegation pool

Use this command to specify the local prefix pool for the DHCPv6 server.

Use the **no** form of this command to restore the default setting.

**prefix-delegation pool** *poolname [ lifetime { valid-lifetime | preferred-lifetime } ]*  
**no prefix-delegation pool** *poolname*

Parameter	Description
-----------	-------------

<b>Parameter Description</b>	<i>poolname</i>	Sets the local prefix pool name.
	<b>lifetime</b>	Sets the lifetime of the address prefix allocated to the client. With the keyword <b>lifetime</b> configured, both parameters <i>valid-lifetime</i> and <i>preferred-lifetime</i> shall be configured.
	<i>valid-lifetime</i>	Sets the valid lifetime of using the allocated address prefix for the client.
	<i>preferred-lifetime</i>	Sets the preferred lifetime of the address prefix allocated to the client.

**Defaults** By default, no address prefix pool is specified.  
The default *valid-lifetime* is 3600s(1 hour).  
The default *preferred-lifetime* is 3600s(1 hour).

**Command Mode** DHCPv6 pool configuration mode

**Usage Guide** Use the **prefix-delegation pool** command to set the prefix pool for the DHCPv6 Server and allocate the prefix to the client. Use the **ipv6 local pool** command to set the prefix pool.  
The Server attempts to allocate a usable prefix from the prefix pool to the client upon receiving the prefix request from the client. That prefix will be allocated to other clients if the client no longer uses that prefix again.

**Configuration** The following example specifies the local prefix pool for the DHCPv6 server.

```

Examples
Hostname(config)# ipv6 dhcp pool pool1
Hostname(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime
2000 1000

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipv6 dhcp pool</b>	Sets a DHCPv6 pool.
	<b>ipv6 local pool</b>	Sets a local prefix pool.
	<b>prefix-delegation</b>	Statically binds the client with the address prefix.
	<b>show ipv6 dhcp pool</b>	Displays the DHCPv6 pool information.

**Platform Description** N/A

## 1.14 show ipv6 dhcp

Use this command to display the device DUID.

**show ipv6 dhcp**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode/Interface configuration mode/Global configuration mode				
<b>Usage Guide</b>	The server, client and relay on the same device share a DUID.				
<b>Configuration Examples</b>	The following example displays the device DUID. <pre> Hostname# show ipv6 dhcp This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0 </pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
<b>Platform Description</b>	N/A				

## 1.15 show ipv6 dhcp binding

Use this command to display the address binding information for the DHCPv6 server.

**show ipv6 dhcp binding** [ *ipv6-address* ]

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ipv6-address</i></td> <td>Sets the IPv6 address or the prefix.</td> </tr> </tbody> </table>	Parameter	Description	<i>ipv6-address</i>	Sets the IPv6 address or the prefix.
Parameter	Description				
<i>ipv6-address</i>	Sets the IPv6 address or the prefix.				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	If the <i>ipv6-address</i> is not specified, all prefixes dynamically assigned to the client and IANA address binding information are shown. If the <i>ipv6-address</i> is specified, the binding information for the specified address is shown.				
<b>Configuration Examples</b>	The following example displays the address binding information for the DHCPv6 server. <pre> Hostname# show ipv6 dhcp binding Client DUID: 00:03:00:01:00:d0:f8:22:33:ac IAPD: iaid 0, T1 1800, T2 2880 Prefix: 2001:20::/72         preferred lifetime 3600, valid lifetime 3600         expires at Jan 1 2008 2:23 (3600 seconds) </pre>				

Related	Command	Description
Commands	N/A	N/A

Platform N/A  
Description

## 1.16 show ipv6 dhcp conflict

Use this command to display the DHCPv6 address conflicts.

**show ipv6 dhcp conflict**

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Command Privileged EXEC mode  
Mode

Usage Guide N/A

**Configuration** The following example displays the DHCPv6 address conflicts.

**Examples**

```

Hostname# show ipv6 dhcp conflict
2008:50::2    declined
2108:50::2    declined
2008:50::3    declined
2008:50::4    declined
2108:50::4    declined
2008:50::5    declined

```

Related	Command	Description
Commands	<b>clear ipv6 dhcp conflict</b>	Clears address conflicts.

Platform N/A  
Description

## 1.17 show ipv6 dhcp interface

Use this command to display the DHCPv6 interface information.

**show ipv6 dhcp interface** [ *interface-name* ]

Parameter	Description
-----------	-------------

<b>Parameter Description</b>	<i>interface-name</i>	Sets the interface name.
------------------------------	-----------------------	--------------------------

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the *interface-name* is not specified, all DHCPv6 interface information is displayed. If the *interface-name* is specified, the specified interface information is displayed.

**Configuration** The following example displays the server-based DHCPv6 interface information.

**Examples**

```

Hostname# show ipv6 dhcp interface
VLAN 1 is in server mode
  Server pool dhcp-pool
  Rapid-Commit: disable

```

The following example displays the client-based DHCPv6 interface information.

```

Hostname# show ipv6 dhcp interface
FastEthernet 0/1 is in client mode
  Rapid-Commit: disable

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Platform Description** N/A

## 1.18 show ipv6 dhcp pool

Use this command to display the DHCPv6 pool information.

**show ipv6 dhcp pool** [ *poolname* ]

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>poolname</i>	Defines the DHCPv6 pool name.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If the *poolname* is not specified, all DHCPv6 interface information is displayed. If the *poolname* is specified, the specified interface information is displayed.

**Configuration** The following example displays the DHCPv6 pool information.

**Examples**

```

Hostname# show ipv6 dhcp pool
DHCPv6 pool: dhcp-pool
  DNS server: 2011:1::1
  DNS server: 2011:1::2
  Domain name: example.com
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.19 show ipv6 dhcp server statistics

Use this command to display the DHCPv6 server statistics.

**show ipv6 dhcp server statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the DHCPv6 server statistics.

**Configuration** The following example displays the DHCPv6 server statistics.

```

Examples Hostname# show ipv6 dhcp server statistics
DHCPv6 server statistics:

Packet statistics:
DHCPv6 packets received:          7
Solicit received:                  7
Request received:                  0
Confirm received:                  0
Renew received:                    0
Rebind received:                   0
Release received:                  0
Decline received:                  0
Relay-forward received:            0
Information-request received:      0
Unknown message type received:     0
Error message received:            0

DHCPv6 packet sent:                0
Advertise sent:                    0
Reply sent:                         0
Relay-reply sent:                  0
Send reply error:                  0
Send packet error:                 0

Binding statistics:
Bindings generated:                0
IAPD assigned:                     0
IANA assigned:                     0

Configuration statistics:
DHCPv6 server interface:           1
DHCPv6 pool:                        0
DHCPv6 iapd binding:               0
    
```

Related Commands	Command	Description
	<b>ipv6 dhcp pool</b>	Sets a DHCPv6 pool.

**Platform** N/A  
**Description**

## 1.20 show ipv6 local pool

Use this command to display the local prefix pool configuration and usage.

**show ipv6 local pool** [*poolname* ]

Parameter	Parameter	Description
Description	<i>poolname</i>	The local prefix pool name

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the local prefix pool configuration and usage.

**Configuration Examples** The following example displays all local prefix pool information.

```

Hostname#show ipv6 local pool
Pool                Prefix
Free                In use
client-prefix-pool  2001:db8::/64
65536                0
    
```

Field	Description
Pool	The local address pool name.
Prefix	The prefix and prefix length.
Free	The available prefix.
In use	The prefix in use.

The following example displays the information about the specified local prefix pool.

```

Hostname#show ipv6 local pool client-prefix-pool
Prefix is 2001:db8::/64 assign /80 prefix
1 entries in use, 65535 available
Prefix                Interface
2001:db8::/80         GigabitEthernet
0/0
    
```

Field	Description
Prefix	The assigned prefix and prefix length.
Interface	The assigning interface.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A



# 1 ND Proxy Commands

## 1.1 clear proxy-nd

Use this command to clear a specified proxy ND entry or all proxy ND entries.

**clear proxy-nd** [ [ *ipv6-address* *vlan-id* ] | *vlan-id* ]

Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the IP address of the proxy ND entry. By default, all proxy ND entries are cleared.
	<i>vlan-id</i>	VLAN ID. The range is from 1 to 4094.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can clear a specified proxy ND entry or all proxy ND entries.

**Configuration Examples** The following example clears all proxy ND entries.

```
Hostname# clear proxy-nd
```

The following example clears a specified proxy ND entry.

```
Hostname# clear proxy-nd 2000::2 2
```

The following example clears all proxy ND entries in VLAN 3.

```
Hostname# clear proxy-nd 3
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 proxy-nd

Use this command to configure a static ND proxy entry.

**proxy-nd** *ipv6-address* *vid* *mac* *interface-id*

Use the **no** form of this command to delete the static ND Proxy.

**no proxy-nd ipv6-address vid**

**Parameter Description**

Parameter	Description
<i>ipv6-address</i>	Specifies an IPv6 address.
<i>vid</i>	Specifies a VLAN ID.
<i>mac</i>	Specifies a MAC address.
<i>interface-id</i>	Specifies an interface.

**Defaults**

No static ND proxy is configured by default.

**Command Mode**

Global configuration mode

**Usage Guide**

N/A

**Configuration Examples**

The following example configures a static ND proxy entry.

```
Hostname(config)# proxy-nd 2000::1 2 0001.0001.0001 GigabitEthernet 0/1
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description**

N/A

### 1.3 proxy-nd enable

Use this command to enable Layer-2 ND Proxy.

**proxy-nd enable**

Use the **no** form of this command to disable Layer-2 ND Proxy.

**no proxy-nd enable**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

By default, Layer-2 ND Proxy is enabled.

**Command Mode**

Global configuration mode

**Usage Guide** N/A

**Configuration** The following example disables Layer-2 ND Proxy.

```
Examples Hostname(config)# no proxy-nd enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.4 show proxy-nd

Use this command to display all proxy ND entries.

```
show proxy-nd [ dynamic | static | [ ipv6-address vlan-id ] ]
```

Parameter Description	Parameter	Description
	<b>dynamic</b>	
<b>static</b>		Displays all static proxy ND entries
<i>ipv6-address</i>		Specifies an IPv6 address.
<i>vlan-id</i>		Specifies a VLAN.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all proxy ND entries.

```
Hostname# show proxy-nd
Total Entry:2
IPv6          Vid      Mac                Interface        Type
-----
2000::2      1        0013.20a5.7a5f    Gi0/1            DYNAMIC
2000::3      2        0013.20a5.7a51    Gi0/2            DYNAMIC
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.5 show proxy-nd statistics

Use this command to display statistics about the proxy ND entry.

**show proxy-nd statistics**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can use this command to display statistics about the proxy ND entry, such as: total proxy ND entries, next aging time and dropped packet count.

**Configuration Examples** The following example displays statistics about the proxy ND entry.

```

Hostname# show proxy-nd statistics

Nd Proxy: Enable

Total Entry: 100

Dynamic Entry: 99

Static Entry: 1

Next Aging Time: 5 Seconds

Dropped Packets: 0
    
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

# 1 TCP Commands

## 1.1 ip tcp adjust-mss

Use this command to change the Maximum Segment Size (MSS) option value of SYN packets sent and received on an interface. Use the **no** form of this command to restore the default setting.

**ip tcp adjust-mss** *max-segment-size*

**no ip tcp adjust-mss**

Parameter Description	Parameter	Description
	<i>max-segment-size</i>	Maximum segment size in the range from 500 to 1460 bytes

**Defaults** The MSS option value of SYN packets is not changed by default.

**Command Mode** Interface configuration mode

**Usage Guide** MSS refers to the maximum size of the payload of a TCP packet. The TCP Path MTU (PMTU) is implemented as per RFC1191. This feature can improve the network bandwidth utilization ratio. When the user uses TCP to transmit mass data, this feature can substantially enhance the transmission performance.

When the client initiates a TCP connection, it negotiates the maximum payload of TCP packets through the MSS option field of the TCP SYN packet. The MSS value of the client's SYN packet implies the maximum payload of TCP packets sent by the server, and vice versa.

Configuring this command on the interface will change the MSS option of SYN packets received or sent by the interface to the MSS value configured on the interface. If the MSS is configured on both the inbound interface and the outbound interface of the SYN packet, the smaller of the two applies. It is recommended that you configure the same value on the inbound interface and outbound interface. This command actually changes the SYN packet exchanged during TCP connection establishment. For some versions, this command may also change the SYN+ACK packet.

This command takes effect on the subsequent TCP connections to be established instead of established TCP connections.

**Configuration Examples** The following example changes the MSS option value of the TCPv4 SYN packet to 1000 bytes on port GigabitEthernet 0/1.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip tcp adjust-mss 1000

```

Related Commands	Command	Description
------------------	---------	-------------

N/A	N/A
-----	-----

**Platform** N/A

**Description**

## 1.2 ip tcp keepalive

Use this command to enable the TCP keepalive function.

**ip tcp keepalive** [ **interval** *num1* ] [ **times** *num2* ] [ **idle-period** *num3* ]

**Parameter Description**

Parameter	Description
<b>interval</b> <i>num1</i>	The interval of sending the keepalive packet, in the range from 1 to 120 in the unit of seconds, The default is 75.
<b>times</b> <i>num2</i>	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
<b>idle-period</b> <i>num3</i>	Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900.

**Defaults** The function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The keepalive function enables TCP to detect whether the peer end is operating properly. Suppose the keepalive function is enabled together with default **interval**, **times** and **idle-period** settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example enables the TCP keepalive function on the device and sets the **idle-period** and **interval** to 180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid.

```
Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** When you run the RGOS 10.x command **service tcp-keepalives-in** or **service tcp-keepalives-out**, it is converted to this command automatically in RGOS 11.0.

## 1.3 ip tcp mss

Use this command to set the upper limit of the MSS value. Use the **no** form of this command to restore the default setting.

**ip tcp mss** *max-segment-size*

**no ip tcp mss**

Parameter Description	Parameter	Description
	<i>max-segment-size</i>	Upper limit of the MSS value in the range from 68 to 10000 bytes

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general.

**Configuration Examples** The following example sets the upper limit of the MSS value to 1300 bytes.

```
Hostname(config)# ip tcp mss 1300
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 1.4 ip tcp path-mtu-discovery

Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the **no** form of this command to restore the default setting.

**ip tcp path-mtu-discovery** [ **age-timer** *minutes* | **age-timer infinite** ]

**no ip tcp path-mtu-discovery**

Parameter Description	Parameter	Description
	<b>age-timer</b> <i>minutes</i>	The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10.
	<b>age-timer infinite</b>	No further discovery after discovering PMTU

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch.

Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled.

According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter **age-timer**. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval until the PMTU value reaches the MSS or the user stops this timer. Use the parameter **age-timer infinite** to stop this timer.

**Configuration** The following example enables PMTU discovery.

**Examples**

```
Hostname(config)# ip tcp path-mtu-discovery
```

**Related Commands**

Command	Description
<b>show tcp pmtu</b>	Shows the PMTU value for the TCP connection.

**Platform Description** In versions 10.X, this command applies to both IPv4 and IPv6 TCP. In version 11.0 or later, this command only applies to IPv4 TCP, and PMTU discovery function is always enabled and cannot be disabled.

## 1.5 ip tcp send-reset

Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the **no** form of this command to disable this function,

**ip tcp send-reset**

**no ip tcp send-reset**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode



**Usage Guide** In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found. However, flooding TCP port unreachable packets pose an attack threat to the device. This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet.

```
Hostname(config)# no ip tcp send-reset
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** The **ip tcp not-send-rst** command in RGOS 10.x is compatible in RGOS 11.0. When you run this command, it is converted to the **no ip tcp send-reset** command automatically.

## 1.6 ip tcp synwait-time

Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the **no** form of this command to restore the default setting.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time** *seconds*

**Parameter Description**

Parameter	Description
<i>seconds</i>	Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds.

**Defaults** The default is 20.

**Command Mode** Global configuration mode

**Usage Guide** If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.

**Configuration Examples** The following example set the timeout value for SYN packets to 10 seconds.

```
Hostname(config)# ip tcp synwait-time 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 1.7 ip tcp window-size

Use this command to change the size of receiving buffer and sending buffer for TCP connections. Use the **no** form of this command to restore the default setting.

**ip tcp window-size** *size*

**no ip tcp window-size**

Parameter Description	Parameter	Description
	<i>size</i>	

**Defaults** The default is 65535.

**Command Mode** Global configuration mode

**Usage Guide** The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.

When the window size exceeds 65,535 bytes, the size of receiving buffer is increased automatically.

**Configuration Examples** The following example sets the TCP window size to 16,386 bytes.

```
Hostname(config)# ip tcp window-size 16386
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** In versions 10.X, this command only applies to IPv4 TCP. In version 11.0 or later, this command applies to both IPv4 and IPv6 TCP.

## 1.8 ipv6 tcp adjust-mss

Use this command to set the MSS option value of the TCPv6 SYN packet. Use the **no** form of this command to restore the default setting.

**ipv6 tcp adjust-mss** *max-segment-size*

**no ipv6 tcp adjust-mss**

### Parameter Description

Parameter	Description
<i>max-segment-size</i>	The maximum segment size (MSS), in the range from 1220 to 1440 in the unit of bytes.

### Defaults

The MSS option value of the TCPv6 SYN packet is not changed by default.

### Command

Interface configuration mode

### Mode

### Usage Guide

TCP negotiates MSS at 3-way handshake. If the IPv6 MTU of one link for TCPv6 packet transmission is too small and packet segmentation is not allowed during forwarding, the device changes the MSS option value of the TCPv6 SYN packet to prevent transmitting the TCPv6 packet surpassing MTU.

This configuration is not applicable to established TCPv6 connections.

### Configuration Examples

The following example sets the MSS option value of the TCPv6 SYN packet to 1300 bytes on port GigabitEthernet 0/1.

```

Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 tcp adjust-mss 1300

```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.9 show ipv6 tcp connect

Use this command to display the current IPv6 TCP connection information.

**show ipv6 tcp connect** [ **local-ipv6** X:X:X:X::X ] [ **local-port** *num* ] [ **peer-ipv6** X:X:X:X::X ] [ **peer-port** *num* ]

Use this command to display the current IPv6 TCP connection statistics.

**show ipv6 tcp connect statistics**

### Parameter

Parameter	Description
-----------	-------------

<b>Description</b>	
<b>local-ipv6</b> X:X:X:X::X	Local IPv6 address
<b>local-port</b> num	Local port
<b>peer-ipv6</b> X:X:X:X::X	Peer IPv6 address
<b>peer-port</b> num	Peer port
<b>statistics</b>	Displays IPv6 TCP connection statistics

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the current IPv6 TCP connection information.

**Examples**

```

Hostname#show ipv6 tcp connect
Number Local Address      Foreign Address      State      Process name
1      :::22                :::0                LISTEN     rg-sshd
2      :::23                :::0                LISTEN     rg-telnetd
3      1000::1:23          1000::2:64201      ESTABLISHED rg-telnetd
    
```

The following example displays the current IPv6 TCP connection statistics.

```

Hostname#show ipv6 tcp connect statistics
State      Count
-----
ESTABLISHED 1
SYN_SENT   0
SYN_RECV   0
FIN_WAIT1  0
FIN_WAIT2  0
TIME_WAIT  0
CLOSED     0
CLOSE_WAIT 0
LAST_ACK   0
LISTEN     1
CLOSING    0
Total: 2
    
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Platform** N/A

**Description**

## 1.10 show ipv6 tcp pmtu

Use this command to display information about IPv6 TCP PMTU.

**show ipv6 tcp pmtu** [ **local-ipv6** X:X:X:X::X ] [ **local-port** num ] [ **peer-ipv6** X:X:X:X::X ] [ **peer-port** num ]

Parameter Description	Parameter	Description
	<b>local-ipv6</b> X:X:X:X::X	Local IPv6 address
	<b>local-port</b> num	Local port
	<b>peer-ipv6</b> X:X:X:X::X	Peer IPv6 address
	<b>peer-port</b> num	Peer port

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example information about IPv6 TCP PMTU.

```

Hostname# show ipv6 tcp pmtu
Number  Local Address          Foreign Address          PMTU
1       1000:::1:23             1000:::2.13560
    
```

Field	Description
Number	Number
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
PMTU	Path MTU.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.11 show ipv6 tcp port

Use this command to display the current IPv6 TCP port status.

**show ipv6 tcp port [ num ]**

Parameter Description	Parameter	Description
	<i>num</i>	Port number

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the current IPv6 TCP port status.

**Examples**

```

Hostname# show ipv6 tcp port
TCP connections on port 23:
Number Local Address Foreign Address State
1      1000::1:23    1000::2:64571 ESTABLISHED
Total: 1

TCP connections on port 2650:
Number Local Address Foreign Address State
Total: 0
    
```

Field	Description
Number	Number
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

State	<p>Current status of the TCP connection. There are eleven possible states:</p> <p>CLOSED: The connection has been closed.</p> <p>LISTEN: Listening state</p> <p>SYNSENT: In the three-way handshake phase when the SYN packet has been sent out.</p> <p>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.</p> <p>ESTABLISHED: The connection has been established.</p> <p>FINWAIT1: The local end has sent the FIN packet.</p> <p>FINWAIT2: The FIN packet sent by the local end has been acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</p>
Process Name	Process name

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.12 show tcp connect

Use this command to display basic information about the current TCP connections.

**show tcp connect** [ **local-ip** *a.b.c.d* ] [ **local-port** *num* ] [ **peer-ip** *a.b.c.d* ] [ **peer-port** *num* ]

Use this command to display the current IPv4 TCP connection statistics.

**show tcp connect statistics**

**Parameter Description**

Parameter	Description
<b>local-ip</b> <i>a.b.c.d</i>	Local IP address.
<b>local-port</b> <i>num</i>	Local port.
<b>peer-ip</b> <i>a.b.c.d</i>	Peer IP address.
<b>peer-port</b> <i>num</i>	Peer port.

<b>statistics</b>	Displays IPv4 TCP connection statistics.
-------------------	--

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the current IPv4 TCP connection information.

**Examples**

```

Hostname# show tcp connect
Number Local Address      Foreign Address      State      Process name
1      0.0.0.0:22              0.0.0.0:0           LISTEN     rg-sshd
2      0.0.0.0:23              0.0.0.0:0           LISTEN     rg-telnetd
3      1.1.1.1:23              1.1.1.2:64201      ESTABLISHED rg-telnetd
    
```

Field	Description
Number	Sequence number.
Local Address	The Local address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23”, “23” is the port number.
Foreign Address	The remote address and port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23”, “23” is the port number.
State	<p>Current status of the TCP connection. There are eleven possible states:</p> <p>CLOSED: The connection has been closed.</p> <p>LISTEN: Listening state</p> <p>SYNSENT: In the three-way handshake phase when the SYN packet has been sent out.</p> <p>SYNRCVD: In the three-way handshake phase when the SYN packet has been received.</p> <p>ESTABLISHED: The connection has been established.</p> <p>FINWAIT1: The local end has sent the FIN packet.</p> <p>FINWAIT2: The FIN packet sent by the local end has been acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been</p>



	acknowledged, and the local end has also acknowledged the FIN packet.
Process name	Process name.

The following example displays the current IPv4 TCP connection statistics.

```

Hostname#show tcp connect statistics
State          Count
-----
ESTABLISHED   1
SYN_SENT      0
SYN_RECV      0
FIN_WAIT1     0
FIN_WAIT2     0
TIME_WAIT     0
CLOSED        0
CLOSE_WAIT    0
LAST_ACK      0
LISTEN        1
CLOSING       0
Total: 2
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.13 show tcp parameter

Use this command to show TCP parameters.

**show tcp parameter**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example shows TCP parameters.

**Examples**

```

Hostname# show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit:
bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit:
bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
  Max SYN retries: 5
  Max SYN ACK retries: 5
Timewait specific information:
  Max timewait sockets: 180000
  Current timewait sockets: 0
  Timewait recycle: 0
  Reuse timewait port: 0
Keepalive information:
  Keepalive on: 0
  Idle period: 900 seconds
  Interval: 75 seconds
  Max probes: 6
MTU probing:
  Enable mtu probing: 0
FIN specific information:
  FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
  Max orphans: 16384
  Max orphan retries: 0
Current orphans: 0
    
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

## 1.14 show tcp pmtu

Use this command to display information about TCP PMTU.

```
show tcp pmtu [ local-ip a.b.c.d ] [ local-port num ] [ peer-ip a.b.c.d ] [ peer-port num ]
```

Parameter Description	Parameter	Description
	<b>local-ip</b> <i>a.b.c.d</i>	Local IP address.
	<b>local-port</b> <i>num</i>	Local port.
	<b>peer-ip</b> <i>a.b.c.d</i>	Peer IP address.
	<b>peer-port</b> <i>num</i>	Peer port.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays PMTU of IPv4 TCP connection.

### Examples

```
Hostname# show tcp pmtu
Number  Local Address          Foreign Address          PMTU
1       192.168.195.212.23     192.168.195.112.13560  1440
```

Field	Description
Number	Sequence number.
Local Address	The local address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
Foreign Address	The remote address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
PMTU	PMTU value.

Related Commands	Command	Description
	<b>ip tcp path-mtu-discovery</b>	Enables the TCP PMTU discovery function.

**Platform Description** N/A

## 1.15 show tcp port

Use this command to display information about the current TCP port.

**show tcp port** [ *num* ]

Parameter Description	Parameter	Description
	<i>num</i>	Port number

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the current IPv4 TCP port status.

### Examples

```

Hostname# show tcp port
TCP connections on port 23:
Number  Local Address  Foreign Address  State
1       1.1.1.1:23     1.1.1.2:64571   ESTABLISHED
Total: 1

TCP connections on port 2650:
Number  Local Address  Foreign Address  State
Total: 0

```

Tcpv6 listen on 23 have total 1 connections.

Field	Description
Number	Port number
Local Address	Local address
Foreign Address	Remote address
State	Status of the current TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been

	<p>acknowledged.</p> <p>CLOSEWAIT: The local end has received the FIN packet from the peer end.</p> <p>LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet.</p> <p>CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received.</p> <p>TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</p>
--	--

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.16 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.  
**show tcp statistics**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example shows TCP parameters.

**Examples**

```

Hostname# show tcp statistics
TCP Packets
  Received: 1103
  Errors : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
    
```

```

Accept backlog full: 0
Web authentication limit per user: 0
Failed to alloc memory for request sock: 0
Failed to create open request child: 0
SYN ACK retransmits: 0
Timeouted requests: 0
Time-wait
Time-wait bucket table overflow: 0
    
```

Field Description

Field	Description
TCP Packets	Normal packets and error packets
Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
Time-wait	Session in TIMEWAIT state

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

# 1 IP REF Commands

## 1.1 clear ip ref packet statistics

Use this command to clear IPv4 Ruijie Express Forwarding (REF) packet statistics.

### clear ip ref packet statistics

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example clears IPv4 REF packet statistics.	
	<pre>Hostname# clear ip ref packet statistics</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.2 clear ipv6 ref packet statistics

Use this command to clear IPv6 REF packet statistics.

### clear ipv6 ref packet statistics

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	

**Configuration** The following example clears IPv6 REF packet statistics.

**Examples**

```
Hostname# clear ipv6 ref packet statistics
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.3 ip ref load-sharing original

Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv4 addresses. Use the **no** form of this command to restore the default setting.

**ip ref load-sharing { original | original-only }**

**no ip ref load-sharing { original | original-only }**

Parameter Description	Parameter	Description
	<b>original -</b>	Sets the load balancing algorithm of IPv4 REF to load balancing based on the source and destination IP addresses.
	<b>original-only</b>	Sets the load balancing algorithm of IPv4 REF to load balancing based on the source IP address.

**Defaults** The default algorithm is based on the destination IPv4 address.

**Command** Global configuration mode

**Mode**

**Usage Guide** The REF is responsible for data forwarding and supports two load balancing algorithms. One is based on destination IP addresses and the other is based on the source and destination IP addresses. When IP packets are forwarded on multiple paths, for example, when load balancing based on destination IP addresses is configured, the REF forwards packets based on a path matching the destination IP address of packets. By default, load balancing based on destination IP addresses is used.

**Configuration** The following example configures the load balancing algorithm based on source and destination IP addresses.

**Examples**

```
Hostname(config)# ip ref load-sharing original
```

The following example configures the load balancing algorithm based on destination IP addresses of packets.

```
Hostname(config)# no ip ref load-sharing original
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A



## Description

## 1.4 ipv6 ref load-sharing original

Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv6 addresses. Use the **no** form of this command to restore the default setting.

**ipv6 ref load-sharing original**

**no ipv6 ref load-sharing original**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** The default algorithm is based on the destination IPv6 address.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example restores the algorithm that is used for load balancing during forwarding to the default setting.

```
Hostname(config)# no ipv6 ref load-sharing original
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A.

**Description**

## 1.5 show ip ref adjacency

Use this command to display the information about the specified adjacent node or all adjacent nodes.

**show ip ref adjacency [ glean | local | ip-address | interface interface\_type interface\_number | discard | statistics ]**

Parameter	Parameter	Description
Description	<b>glean</b>	Aggregate adjacent node, which is used for a direct route
	<b>local</b>	Local adjacent node, which is used by the local host
	<i>ip</i>	Next-hop IP address
	<i>interface_type</i>	Interface type
	<i>interface_number</i>	Interface number
	<b>discard</b>	Displays discarded adjacent nodes.
	<b>statistics</b>	Statistics

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.

**Configuration** The following example displays the information about all adjacent nodes in the adjacent node table.

**Examples**

```

Hostname#show ip ref adjacency
id state      type    rfct chg ip                interface          linklayer(header
data)
1  unresolved mcast  1    0  224.0.0.0
9  resolved   forward 1    0  192.168.50.78 GigabitEthernet 0/1  00 25 64 C5
9D 6A 00 D0 F8 98 76 54 08 00
7  resolved   forward 1    0  192.168.50.200 GigabitEthernet 0/1  00 04 5F 87
69 66 00 D0 F8 98 76 54 08 00
6  unresolved glean  1    0  0.0.0.0          GigabitEthernet 0/1
4  unresolved local  3    0  0.0.0.0          Local 1

```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

**Related Commands**

Command	Description
show ip ref route	Displays all route information in the current REF module.

**Platform** N/A  
**Description**

## 1.6 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

**show ip ref exact-rout** *source\_ipaddress destination\_ipaddress*

Parameter	Parameter	Description
Description	<i>source_ipaddress</i>	Source IP address of the packet
	<i>destination_ipaddress</i>	Destination IP address of the packet

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF

**Configuration Examples** The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

```

Hostname# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74 --> 192.168.13.1 (vrf global):
id state type rfct chg ip interface linklayer(header
data)
9 resolved forward 1 0 192.168.17.1 GigabitEthernet 0/1 00 25 64 C5 9D
6A 00 D0 F8 98 76 54 08 00
    
```

Description of fields:

Field	Description
id	Adjacency ID
state	Adjacency state: Unresolved Resolved
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacency
chg	Whether the adjacency is on the changing link.

ip	Adjacency IP address
interface	Interface
linklayer	Layer 2 head

Related	Command	Description
Commands	<b>show ip ref route</b>	Displays all routing information in the current REF module.

**Platform** N/A  
**Description**

## 1.7 show ip ref packet statistics

Use this command to display IPv4 REF packet statistics.

**show ip ref packet statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv4 REF packet statistics.

```
Ruijie #show ip ref pkt-statistic
ref packet statistic:
  bad head      : 0
  lookup fib fail : 0
  local adj     : 0
  glean adj     : 0
  forward      : 0
  redirect     : 0
  punt adj     : 0
  outif not in ef : 0
  ttl expiration : 0
  no ip routing  : 0
```

Field	Description
total recved	Number of total packets received by REF
bad head	Number of the packets with false header

lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.8 show ip ref resolve-list

Use this command to display the IPv4 REF resolution information.

**show ip ref resolve-list**

**Parameter**  
**Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays IPv4 REF resolution information.

**Examples**

```

Hostname# show ip ref resolve-list
IP                res_state flags interface
1.1.1.1           unres    1    GigabitEthernet 0/1
    
```

Field	Description
IP	IP address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

**show ip ref route** [ **default** | *ip-address mask* | **statistics** ]

Parameter Description	Parameter	Description
	<b>default</b>	Specifies the default route.
	<i>ip-address</i>	Specifies the destination IP address of the route
	<i>mask</i>	Specifies the mask of the route.
	<b>statistics</b>	Statistics

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.

**Configuration Examples** The following example displays all the routing information in the IPv4 REF table.

```

Hostname# show ip ref route
Codes: * - default route
       # - zero route
ip      mask      weight path-id  next-hop  interface
255.255.255.255 255.255.255.255 1 4 0.0.0.0 Local 0
224.0.0.0      240.0.0.0      1 1 224.0.0.0
224.0.0.0      255.255.255.0  1 4 0.0.0.0 Local 0
192.168.50.0   255.255.255.0   1 6 0.0.0.0 FastEthernet 0/1
192.168.50.255 255.255.255.255 1 2 0.0.0.0
192.168.50.200 255.255.255.255 1 7 192.168.50.200 FastEthernet 0/1
192.168.50.122 255.255.255.255 1 4 0.0.0.0 Local 0
192.168.50.78 255.255.255.255 1 9 192.168.50.78 FastEthernet 0/1

```

Field	Description
ip	Destination IP address
mask	Mask

path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Egress

**Related  
Commands**

Command	Description
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.

**Platform** N/A

**Description**

## 1.10 show ipv6 ref adjacency

Use this command to display the information about the IPv6 adjacent node.

**show ipv6 ref adjacency** [**glean** | **local** | *ipv6-address* | **interface** *interface\_type interface\_number* | **discard** | **statistics** ]

**Parameter  
Description**

Parameter	Description
<b>glean</b>	Aggregate adjacent node, which is used for a direct route
<b>local</b>	Local adjacent node, which is used by the local host
<i>ipv6-address</i>	Next-hop IP address
<i>interface_type</i>	Interface type
<i>interface_number</i>	Interface number
<b>discard</b>	Displays discarded adjacent nodes.
<b>statistics</b>	Statistics

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.

**Configuration** The following example displays the information about the IPv6 adjacent node.

**Examples**

```

Hostname# show ipv6 ref adjacency
id  state      type  rfct chg ip  interface          linklayer (header
data)
1   unresolved glean  1    0   ::  GigabitEthernet 0/1
2   unresolved local   2    0   ::1 Local 1

```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.

Related Commands	Command	Description
	N/A	N/A

Platform  
Description

N/A

## 1.11 show ipv6 ref exact-route

This command is used to display the IPv6 REF exact route.

**show ipv6 ref exact-route** *source-ipv6-address destination-ipv6-address*

Parameter Description	Parameter	Description
	<i>source-ipv6-address</i>	Source IP address of the packet
	<i>destination-ipv6-address</i>	Destination IP address of the packet

Defaults

N/A

Command Mode

Privileged EXEC mode



**Usage Guide** N/A

**Configuration** The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.

**Examples**

```

Hostname# show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2
2001:db8:1::1 --> 3001:db8:2::2 (vrf global):
ID state      type    rfct chg ip interface          linklayer(header data)
3  unresolve  glean  1    0  :: GigabitEthernet 0/1

```

Description of fields:

Field	Description
id	Adjacent node ID
state	Adjacent node state: Unresolved Resolved
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
rfct	Reference count of the adjacent node
chg	Whether the adjacent node is on the changing link.
ip	IP address of the adjacent node
interface	Interface
linklayer	Layer 2 head

For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.12 show ipv6 ref packet statistics

Use this command to display IPv6 REF packet statistics.

**show ipv6 ref packet statistics**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	
	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays IPv6 REF packet statistics.

**Examples**

```

Hostname# show ipv6 ref packet statistics
ref packet statistic:
  bad head      : 0
  lookup fib fail : 0
  local adj     : 0
  glean adj     : 0
  forward      : 0
  redirect      : 0
  hop-limit expiration : 0
  no ipv6 unicast-routing : 0
    
```

Field	Description
total recved	Number of total packets received by REF
bad head	Number of the packets with false header
lookup fib fail	Number of the packets with failed REF routing
drop adj	Number of the packets matching the dropped adjacency
local adj	Number of the packets matching the local adjacency
glean adj	Number of the packets matching the gleaned adjacency
forward	Number of the packets matching the forwarded adjacency
no ip routing	Number of the packets not allowed to be forwarded and sent to local.

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.13 show ipv6 ref resolve-list

This command is used to display the IPv6 REF resolution information.

**show ipv6 ref resolve-list**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays IPv6 REF resolution information.

```

Hostname# show ipv6 ref resolve-list
IP          res_state flags interface
1000::1    unres     1    GigabitEthernet 0/1
    
```

Field	Description
IP	IPv6 address
res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency
interface	Interface

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.14 show ipv6 ref route

Use this command to display all the routing information in the IPv6 REF table.

**show ipv6 ref route [ default | statistics | prefix/len ]**

Parameter Description	Parameter	Description
	<b>oob</b>	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	<b>vrf</b> <i>vrf-name</i>	VRF name, supported only by the VRF-supported device.
	<b>default</b>	Specifies the default route.
	<b>statistics</b>	Statistics
	<b>prefix/len</b>	Displays the route with the specified prefix (X:X:X:X:/<0-128>).

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The command can also be used to display information about the default route, the route with the specified prefix, and statistics of all types of routes.

**Configuration Examples** The following example displays all the routing information in the REF IPv6 table.

```

Hostname# show ipv6 ref route
Codes: * - default route
prefix/len          weight path_id next_hop interface
2001:da8:ffe:2::/64      1      3      ::      GigabitEthernet 0/1
2001:da8:ffe:2::3/128    1      2      :::1    Local 1
fe80::/10             1      6      ::      Null 0
fe80::21a:a9ff:fe3b:fa41/128 1      2      :::1    Local 1

```

Field	Description
prefix/len	IPv6 prefix and prefix length.
path-id	Adjacent identity
next-hop	Address of next hop
weight	Routing weight
interface	Interface

**Related Commands**

Command	Description
---------	-------------

N/A	N/A
-----	-----

**Platform** N/A  
**Description**

# 1 FPM Commands

## 1.1 clear ip fpm counters

Use this command to clear counters about the IPv4 packets.

**clear ip fpm counters**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears counters about the IPv4 packets.

**Examples** `Hostname# clear ip fpm counters`

**Platform Description** N/A

## 1.2 clear ip v6fpm counters

Use this command to clear counters about the IPv6 packets.

**clear ip v6fpm counters**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears counters about the IPv6 packets.

**Examples** `Hostname# clear ip v6fpm counters`

**Platform Description** N/A

## 1.3 ip session direct-trans-disable

Use this command to disable the function to transparently transmit packets when the flow table is full.

**ip session direct-trans-disable**

Use the **no** form of this command to restore the default setting.

**no ip session direct-trans-disable**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	This configuration takes effect only on ACs and APs. With this feature, packets are transparently transmitted instead of establishing any flow on wireless products when the flow table is full, and service processing is not accelerated, thereby ensuring that service flows are not interrupted.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example disables the function to transparently transmit packets when the flow table is full.	
	<pre>Hostname(config)# ip session direct-trans-disable</pre>	
<b>Platform Description</b>	N/A	

## 1.4 ip session tcp-loose

Use this command to enable the loose TCP status transition check function.

**ip session tcp-loose**

Use the **no** form of this command to restore the default setting.

**no ip session tcp-loose**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	By default, the loose TCP status check function is disabled on FW products while enabled on wireless and EG products.	
<b>Command</b>	Global configuration mode	

**Mode****Usage Guide** N/A**Configuration** The following example enables the loose TCP status transition check function.**Examples**

```
Hostname(config)# ip session tcp-loose
```

**Platform****Description** N/A

## 1.5 ip session tcp-state-inspection-enable

Use this command to enable the TCP status tracing function.

**ip session tcp-state-inspection- enable**Use the **no** form of this command to restore the default setting.**no ip session tcp-state-inspection- enable****Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

The TCP status tracing function is disabled on ACs and APs by default.

**Command**

Global configuration mode

**Mode****Usage Guide** N/A**Configuration** The following example enables the TCP status tracing function.**Examples**

```
Hostname(config)# ip session tcp-state-inspection-enable
```

**Platform****Description** N/A

## 1.6 ip session threshold

Use this command to configure the number of packets that can be received for each flow in a certain status.

**ip session threshold { icmp-closed | icmp-started | rawip-closed | tcp-syn-sent | tcp-syn-receive | tcp-closed | udp-closed } { num }**Use the **no** form of this command to restore the default setting.



**no ip session threshold { icmp-closed | icmp-started | rawip-closed | tcp-syn-sent | tcp-syn-receive | tcp-closed | udp-closed }**

**Parameter  
Description**

Parameter	Description
icmp-closed	Sets the number of packets permitted to pass in each ICMP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000.
icmp-started	Sets the number of packets permitted to pass in each ICMP flow in started status, which is 300 by default and ranges from 5 to 2,000,000,000.
rawip-closed	Sets the number of packets permitted to pass in each RAWIP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000.
tcp-syn-sent	Sets the number of packets permitted to pass in each TCP flow in syn-send status, which is 10 by default and ranges from 5 to 2,000,000,000.
tcp-syn-receive	Sets the number of packets permitted to pass in each TCP flow in syn-receive status, which is 20 by default and ranges from 5 to 2,000,000,000.
tcp-closed	Sets the number of packets permitted to pass in each TCP flow in closed status, which is 20 by default and ranges from 5 to 2,000,000,000.
udp-closed	Sets the number of packets permitted to pass in each UDP flow in closed status, which is 10 by default and ranges from 1 to 2,000,000,000.
<i>num</i>	Sets the number of packets permitted to pass.

**Defaults**

**icmp-closed:** 10;  
**icmp-started:** 300;  
**rawip-closed:** 10;  
**tcp-syn-sent:** 10;  
**tcp-syn-receive:** 20;  
**tcp-closed:** 20;  
**udp-closed:** 10.

**Command  
Mode**

Global configuration mode

**Usage Guide**

To activate this configuration, run the **ip session [ dev ] [ slot ] track-state-strictly** command.

**Configuration  
Examples**

The following example configures the number of packets that can be received for each flow in a certain status to 100.

```
Hostname(config)# ip session threshold tcp-closed 100
```

**Platform  
Description**

N/A

## 1.7 ip session timeout

Use this command to configure the aging time.

**ip session timeout { icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin-wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established } { num }**

Use the **no** form of this command to restore the default setting.

**no ip session timeout { icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin-wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established }**

**Parameter Description**

Parameter	Description
icmp-closed	Sets the aging time of ICMP flows in closed status, which is 10 seconds by default and ranges from 5 to 60.
icmp-connected	Sets the aging time of ICMP flows in connected status, which is 10 seconds by default and ranges from 5 to 120.
icmp-started	Sets the aging time of ICMP flows in started status, which is 10 seconds by default and ranges from 5 to 120.
rawip-closed	Sets the aging time of RAWIP flows in closed status, which is 10 seconds by default and ranges from 5 to 60.
rawip-connected	Sets the aging time of RAWIP flows in connected status, which is 300 seconds by default and ranges from 10 to 300.
rawip-established	Sets the aging time of RAWIP flows in established status, which is 300 seconds by default and ranges from 10 to 600.
rawip-started	Sets the aging time of TCP flows in started status, which is 300 seconds by default and ranges from 10 to 300.
tcp-close-wait	Sets the aging time of TCP flows in tcp-close-wait status, which is 60 seconds by default and ranges from 10 to 120.
tcp-closed	Sets the aging time of TCP flows in tcp-closed status, which is 10 seconds by default and ranges from 5 to 20.
tcp-established	Sets the aging time of TCP flows in tcp-established status, which is 1,800 seconds by default and ranges from 300 to 604,800.
tcp-fin-wait1	Sets the aging time of TCP flows in tcp-fin-wait1 status, which is 60 seconds by default and ranges from 10 to 120.
tcp-fin-wait2	Sets the aging time of TCP flows in tcp-fin-wait2 status, which is 60 seconds by default and ranges from 10 to 120.
tcp-syn-receive	Sets the aging time of TCP flows in tcp-syn-receive status, which is 10 seconds by default and ranges from 5 to 30.
tcp-syn-sent	Sets the aging time of TCP flows in tcp-syn-sent status, which is 10 seconds by default and ranges from 5 to 30.
tcp-syn_sent2	Sets the aging time of TCP flows in tcp-syn_sent2 status, which is 10 seconds by default and ranges from 5 to 30.
tcp-time-wait	Sets the aging time of TCP flows in tcp-time-wait status, which is 10 seconds by

	default and ranges from 5 to 60.
udp-closed	Sets the aging time of UDP flows in closed status, which is 10 seconds by default and ranges from 5 to 60.
udp-connected	Sets the aging time of UDP flows in connected status, which is 30 seconds by default and ranges from 10 to 300.
udp-established	Sets the aging time of UDP flows in established status, which is 600 seconds by default and ranges from 120 to 600.
udp-started	Sets the aging time of UDP flows in started status, which is 10 seconds by default and ranges from 10 to 300.
<i>num</i>	Sets the aging time.

**Defaults**

**icmp-closed:** 10 seconds;  
**icmp-connected:** 10 seconds;  
**icmp-started:** 10 seconds;  
**rawip-closed:** 10 seconds;  
**rawip-connected:** 300 seconds;  
**rawip-established:** 300 seconds;  
**rawip-started:** 300 seconds;  
**tcp-close-wait:** 60 seconds;  
**tcp-closed:** 10 seconds;  
**tcp-established:** 1,800 seconds;  
**tcp-fin-wait1:** 60 seconds;  
**tcp-fin-wait2:** 60 seconds;  
**tcp-syn-receive:** 10 seconds;  
**tcp-syn-sent:** 10 seconds;  
**tcp-syn\_sent2:** 10 seconds;  
**tcp-time-wait:** 10 seconds;  
**udp-closed:** 10 seconds;  
**udp-connected:** 30 seconds;  
**udp-established:** 600 seconds;  
**udp-started:** 10 seconds

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the aging time of TCP flows in tcp-established status to 600 seconds.

```

Hostname(config)# ip session timeout tcp-established 600
    
```

**Platform Description** N/A

## 1.8 ip session track-state-strictly

Use this command to configure packet threshold check for flows in various states.

**ip session track-state-strictly**

Use the **no** form of this command to restore the default setting.

**no ip session track-state-strictly**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	This function is disabled by default.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example configures packet threshold check for flows.	
	<pre>Hostname(config)# ip session track-state-strictly</pre>	
<b>Platform Description</b>	N/A	

## 1.9 show ip fpm counters

Use this command to displays the counters about the IPv4 packets.

**show ip fpmcounters**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	Use this command to display the counters about the IPv4 packets, including information about packet loss and flows.	
<b>Configuration Examples</b>	The following example displays the counters about the IPv4 packets.	
	<pre>Hostname# show ip fpm counters Dropped packet counters:</pre>	

```

Count      Reason
0          Non-IPv4 packet
0          Bad IPv4 header length
0          Bad IPv4 total length
0          Fragment pkt
0          change flow state notify FW refuse
0          Bad IPv4 checksum
0          Invalid IPv4 address
0          Invalid TCP flags
0          Invalid TCP sequence
0          Invalid ICMP message type
0          Invalid icmp initial message type
54         Invalid tcp init flags
0          Invalid tcp connection state
0          Connect over config threshold
0          Connect has been terminated
0          Invalid egress fid
0          out of vfw session limit
0          Out of capability
<end>
Rejected or terminated connection counters:
Count      Reason
0          Out of life time
1968       Flow Terminated
0          Rejected by policy
<end>
    
```

**Field Description**

Field	Description
count	Packet counters.
Reason	Packet loss reason.

**Platform** N/A  
**Description**

### 1.10 show ip fpm flows

Use this command to display IPv4 packet flow information.

**show ip fpm flows**

Parameter Description	Parameter	Description
	N/A	N/A

**Command** Privileged EXEC mode

**Mode****Usage Guide** N/A**Configuration** The following example displays IPv4 packet flow information.**Examples**

```

Hostname# show ip fpm flows
Pr SrcAddr                               DstAddr                               SrcPort
DstPort  Vrf           SendBytes RecvBytes  St   srcif
dstif                                ctrl_flag

```

**Field Description**

Field	Description
Pr	Protocol.
SrcAddr	Source address.
DstAddr	Destination address.
SrcPort	Source Port.
DstPort	Destination port.
Vrf	The VRF of the destination interface.
SendBytes	The length of received packets in Tx.
RecvBytes	The length of received packets in Rx.
St	The current state of flows.
srcif	Source interface.
dstif	Destination interface.
ctrl_flag	Flows control flag.

**Platform**

N/A

**Description**

## 1.11 show ip fpm flows filter

Use this command to display IPv4 packet flow information except specific IPv4 packet flows.

**show ip fpm flows filter** *protocol saddr smask daddr dmask*

**Parameter Description**

Parameter	Description
<i>protocol</i>	IP protocol in the range from 0 to 255.
<i>saddr</i>	Source IP addresses.
<i>smask</i>	Source IP mask in the range from 1 to 32.
<i>daddr</i>	Destination IP addresses.
<i>dmask</i>	Destination IP mask in the range from 1 to 32.

**Command** Privileged EXEC mode**Mode****Usage Guide** N/A

**Configuration** The following example displays IPv4 packet flow information except specific IPv4 packet flows.

```

Examples Hostname# show ip fpm flows filter 1 192.168.1.1 32 192.168.2.1 30
Pr SrcAddr DstAddr SrcPort
DstPort Vrf SendBytes RecvBytes St srcif
dstif ctrl_flag
    
```

**Field Description**

Field	Description
Pr	Protocol
SrcAddr	Source address.
DstAddr	Destination address.
SrcPort	Source Port.
DstPort	Destination port.
Vrf	The VRF of the destination interface.
SendBytes	The length of received packets in Tx.
RecvBytes	The length of received packets in Rx.
St	The current state of flows.
srcif	Source interface.
dstif	Destination interface.
ctrl_flag	Flows control flag.

**Platform** N/A  
**Description**

### 1.12 show ip fpm statistics

Use this command to display IPv4 flow statistics.

**show ip fpm statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays IPv4 flow statistics on the EG device.

```

Examples Hostname# show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
    
```

Fpm attribute is eg.

**Field Description**

Field	Description
The capacity of the flow table	The number of total flow tables.
Active flows num	The number of active flow tables.
event count:65,	The counter for current events.
Fpm attribute is eg	The flow tables are generated based on EG products.

**Platform Description** N/A

### 1.13 show ip v6fpm counters

Use this command to displays the counters about the IPv6 packets.

**show ip v6fpm counters**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the counters about the IPv6 packets, including information about packet loss and flows.

**Configuration Examples** The following example displays the counters about the IPv6 packets.

```

Hostname# show ip v6fpm counters
Dropped packet counters:
Count      Reason
0          Non-IPv6 packet
0          Err length
0          Fragment packet
0          Err address
0          Invalid TCP flags
0          Invalid TCP sequence
0          Invalid ICMPV6 message type
0          Invalid ICMPV6 initial message type
0          Invalid tcp init flag
0          Invalid tcp flow state
0          Invalid pkt fid
0          Conn Terminated
    
```



```

0      Out of vfw session limit
0      Out of capability
<end>
Rejected or terminated connection counters:
Count   Reason
0       Out of life time
2105    Flow Terminated
0       Rejected by policy
<end>
    
```

**Field Description**

Field	Description
count	Packet counters.
Reason	Packet loss reason.

**Platform** N/A  
**Description**

### 1.14 show ip v6fpm flows

Use this command to display IPv6 packet flow information.

**show ip v6fpm flows**

Parameter Description	Parameter	Description
	N/A	N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays IPv6 packet flow information.

**Examples**

```

Hostname# show ip v6fpm flows
Pr  Saddr          Daddr
Sport Dport Sedby      Recby      Vrf  st  src_if  dst_id
ctrl_flag
    
```

**Field Description**

Field	Description
Pr	Protocol.
Saddr	Source address.
Daddr	Destination address.
Sport	Source Port.
Dport	Destination port.
Sedby	The length of received packets in Tx.

Recby	The length of received packets in Rx.
Vrf	The VRF of the destination interface.
st	The current state of flows.
sifx	Source interface.
difx	Destination interface.
ctrl_flag	Flows control flag.

**Platform**  
**Description** N/A

## 1.15 show ip v6fpm statistics

Use this command to display IPv6 flow statistics.

### show ip v6fpm statistics

Parameter Description	Parameter	Description
	N/A	N/A

**Command**  
**Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays IPv6 flow statistics.

**Examples**

```

Hostname# show ip v6fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpmv6 state inspection disable.

```

#### Field Description

Field	Description
The capacity of the flow table	The number of total flow tables.
Active flows num	The number of active flow tables.
event count	The counter for current events.

**Platform**  
**Description** N/A



# IP Routing Commands

---

1. IP Routing Basic Commands

# 1 IP Routing Basic Commands

## 1.1 clear ip route

Use this command to clear the route cache.

**clear ip route** { \* | *network* [ *netmask* ] }

Parameter	Description
*	Clears all route cache.
<i>network</i>	Specifies the route cache of the network or subnet.
<i>netmask</i>	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match <i>network</i> with the route. The cache of the longest match is cleared.

**Command Mode** Privileged EXEC mode

**Usage** Clearing route cache clears the corresponding routes and triggers the routing protocol relearning.

**Guide** Please note that clearing all route cache leads to temporary network disconnection.

**Examples** The following example clears the cache of the route which is the longest match with IP address 192.168.12.0.

```
Hostname# clear ip route 192.168.12.0
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.2 ip route

Use this command to configure a static route. Use the **no** or **default** form of this command to restore the default setting.

**ip route** *network net-mask* { *ipv4-address* [ **global** ] | *interface* [ *ipv4-address* [ **global** ] ] } [ *distance* ] [ **tag** *tag* ] [ **permanent** ] [ **weight** *number* ] [ **description** *description-text* ] [ **disabled** | **enabled** ]

**no ip route** *network net-mask* { *ipv4-address* | *interface* [ *ipv4-address* ] } [ *distance* ]

**no ip route all**

**default ip route** *network net-mask* { *ipv4-address* | *interface* [ *ipv4-address* ] } [ *distance* ]

Parameter	Description
<i>network</i>	Network address of the destination
<i>net-mask</i>	Mask of the destination
<i>ipv4-address</i>	The next hop IPv4 address of the static route
<b>global</b>	(Optional) Indicates that the next hop address is global.
<i>interface</i>	(Optional) The next hop egress of the static route
<i>distance</i>	(Optional) The administrative distance of the static route
<b>tag tag</b>	(Optional) The tag of the static route
<b>permanent</b>	(Optional) Permanent route ID
<b>weight number</b>	(Optional) Indicates the weight of the static route. The weight is 1 by default.
<b>description description-text</b>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.
<b>disabled   enabled</b>	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.

**Defaults** No static route is configured by default.

**Command Mode** Global configuration mode

### Usage Guide

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

The default weight of the static route is 1. To view the static route of non default weight, execute the show ip route weight command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries.

Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. When you configure the static route on an Ethernet interface, do not set the next hop as an interface, for example, ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1. In this case, the switch may consider that all unknown destination networks are directly connected to the GigabitEthernet 0/1. So it sends an ARP request to every destination host, which occupies many CPU and memory resources. It is not recommended to set the static route to an Ethernet interface.

### Examples

The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 15.

```
Hostname(config)# ip route 172.16.100.0 255.255.255.0 192.168.12.1 15
```

If the static route has not a specific interface, data flows may be sent through other interface in case

of interface failure. The following example configures data flows to be sent through fastEthernet 0/1 to the destination network of 172.16.100.0/24.

```
Hostname(config)# ip route 172.16.100.0 255.255.255.0 GigabitEthernet 0/1
```

**Related Commands** N/A

**Platform Description** This command is not supported on layer-2 devices.

### 1.3 ip routing

Use this command to enable IP routing in the global configuration mode. Use the **no** or **default** form of this command to disable this function.

- ip routing**
- no ip routing**
- default ip routing**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** IP routing is not necessary when the switch serves as bridge or VoIP gateway. When a device functions only as a bridge or VoIP gateway, the IP routing function of the RGOS software is not required. In this case, the IP routing function of the RGOS software can be disabled. After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the **no ip routing** command, the configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the **no ip routing** command is run. If the **ip routing** command is run again, the static route configuration can be restored.

Note that if the process or whole system restarts when the **no ip routing** command is run, the static route configuration will not be reserved.

**Examples** The following example disables IP routing.

```
Hostname(config)# no ip routing
```

Related Commands	Command	Description
	<code>show ip route</code>	Displays the routing table.

Platform N/A

Description

## 1.4 ip static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**ip static route-limit** *number*

**no ip static route-limit**

**default ip static route-limit**

Parameter	Parameter	Description
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000

Defaults The default is 1024.

Command Global configuration mode  
Mode

Usage Guide The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the **show running-config** command.

Examples The following example sets the upper threshold of the static routes to 900 and then restores the setting to the default value.

```
Hostname(config)# ip static route-limit 900
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

## 1.5 ipv6 route

Use this command to configure an ipv6 static route. Use the **no** or **default** form of this command to restore the default setting.

**ipv6 route** *ipv6-prefix/prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* ] [ **tag** *tag* ] [ **weight** *number* ] [ **description** *description-text* ]

**no ipv6 route** *ipv6-prefix/prefix-length* { *ipv6-address* | *interface* [ *ipv6-address* ] } [ *distance* ]  
**no ipv6 route all**

**Parameter  
Description**

Parameter	Description
<i>ipv6-prefix</i>	Indicates the IPv6 prefix which must comply with the address expression specified in RFC4291
<i>prefix-length</i>	Mask length of the destination
<i>ipv6-address</i>	The next hop IP address of the static route
<i>interface</i>	(Optional) The next hop egress of the static route
<i>distance</i>	(Optional) The administrative distance of the static route. The default is 1.
<b>tag</b> <i>tag</i>	(Optional) The tag value of the static route. The default is 0.
<b>weight</b> <i>number</i>	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio of these routes. The weight is 1 by default.
<b>description</b> <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.

**Defaults** No IPv6 static route is configured by default.

**Command  
Mode** Global configuration mode

**Usage Guide**

The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.

The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115.

```
Hostname(config)# ipv6 route 2001::/64 2002::2 115
```

**Examples**

If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures that data flows are sent through fastEthernet 0/1 to the destination network of 2001::/64.

```
Hostname(config)# ipv6 route 2001::/64 GigabitEthernet 0/1
```

**Related**

Command	Description
---------	-------------



<b>Commands</b>	<b>show ipv6 route</b>	Displays IPv6 routing table.
-----------------	------------------------	------------------------------

**Platform** N/A

**Description**

## 1.6 ipv6 static route-limit

Use this command to set the upper threshold of the static route. Use the **no** or **default** form of this command to restore the default setting.

**ipv6 static route-limit** *number*

**no ipv6 static route-limit**

**default ipv6 static route-limit**

Parameter	Description
<b>Description</b> <i>number</i>	Upper threshold of static routes in the range from 1 to 10000.

**Defaults** The default is 1000.

**Command Mode** Global configuration mode

**Usage Guide** The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

The following example sets the upper threshold of the ipv6 static routes to 900 and then restores the setting to the default value.

### Examples

```
Hostname(config)# ipv6 static route-limit 900
Hostname(config)# no ipv6 static route-limit
```

Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.
	show ipv6 route	Displays the IPv6 routing table.

**Platform** N/A

**Description**

## 1.7 ipv6 unicast-routing

Use this command to enable the IPv6 route function of the RGOS. Use the **no** or **default** form of this command to disable this function.

**ipv6 unicast-routing**  
**no ipv6 unicast-routing**  
**default ipv6 unicast-routing**

	Parameter	Description
Parameter	N/A	N/A
Description	N/A	N/A

**Defaults** This function is enabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

**Examples** The example disables the IPv6 route function of RGOS.  

```
Hostname(config)# no ipv6 unicast-routing
```

	Command	Description
<b>Related Commands</b>	<b>ipv6 route</b>	Configure the IPv6 static route.
	<b>show ipv6 route</b>	Displays the IPv6 routing table.

**Platform Description** N/A

## 1.8 maximum-paths

Use this command to specify the number of equivalent routes. Use the **no** or **default** form of this command is used to restore the default setting.

**maximum-paths** *number*  
**no maximum-paths** *number*  
**default maximum-paths**

	Parameter	Description
Parameter	<i>number</i>	
Description	<i>number</i>	Number of equivalent routes in the range from 1 to 32

**Defaults** The default value is 32

**Command Mode** Global configuration mode

**Usage Guide** The number of equivalent routes is configured to control the number of equivalent routes. After the

number of equivalent routes is configured by running the **maximum-paths** command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes. You can run the **show running config** command to query the number of configured static routes. This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value.

The following example sets the number of equivalent routes to 10 and then restores the default setting.

**Examples**

```

Hostname(config)# maximum-paths 10
Hostname(config)# no maximum-paths 10
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.9 show ip route

Use the commands to display the configuration of the IP routing table.

**show ip route** [ [ *network* [ *mask* [ **longer-prefixes** ] ] | **count** | *protocol* | **weight** ] ]

**show ip route** [ [ **normal** | **ecmp** ] [ *network* [ *mask* ] ]

**Parameter Description**

Parameter	Description
<i>network</i>	(Optional) Displays the route information to the network.
<i>mask</i>	(Optional) Displays the route information to the network of this mask.
<b>longer-prefixes</b>	(optional) Displays the routes that match the specified prefix.
count	(Optional) Displays the number of existent routes (for the ECMP/WCMP route, displays one route).
<i>protocol</i>	(Optional) Displays the route information of specific protocol.
weight	(Optional) Displays the route information of non-default weight.
normal	Displays normal routes and not equivalent routes or fast reroutes.
ecmp	Displays only equivalent routes.

**Defaults** N/A

**Command Mode** All CLI user modes except user EXEC mode

This command can display route information flexibly.

**Usage Guide** This command shows all routes. To show different attributes of routes, specify the normal or ecmp parameter.

The following example displays the configuration of the IP routing table.

```

Hostname# show ip route

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set

S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
    
```

**Examples**

Field	Description
C	Source routing protocol, which may be: C: directly connected route L: local host S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

```

Hostname# show ip route 56.40.0.0
Routing entry for 56.40.0.0/24
    
```

```
Distance 0, metric 0
Routing Descriptor Blocks:
  directly connected, via BVI 1, generated by "connected"
```

Field	Description
Routing Descriptor Blocks	Next hop IP address, source, update time, forwarding interface, source routing protocol and type of route information

```
Hostname# show ip route count
----- route info -----
the num of active route: 5
```

```
Hostname# show ip route weight
-----[distance/metric/weight]-----
S   23.0.0.0/8 [1/0/2] via 192.1.1.20
S   172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
Hostname#show ip route normal

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is no set
S   20.0.0.0/8 is directly connected, VLAN 1
S   22.0.0.0/8 [1/0] via 20.0.0.1
C   192.1.1.0/24 is directly connected, VLAN 1
C   192.1.1.254/32 is local host
```

```
Hostname#show ip route ecmp

Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area, * - candidate default

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*  0.0.0.0/0 [1/0] via 192.168.1.2
      [1/0] via 192.168.2.2
```

## 1.10 show ip route summary

Use this command to display the statistical information about one routing table.

**show ip route summary**

Use this command to display the statistical information about all routing tables.

**show ip route summary all**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** All CLI user modes except user EXEC mode

**Usage guideline** N/A

The following example displays the statistics of the global routing table.

```

Hostname# show ip route summary
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

Memory: 2000 bytes
Entries: 22, based on route prefixes

          NORMAL    ECMP    FRR    TOTAL
Connected 2         0        0        2
Static    1         0        0        1
RIP       0         0        0        0
OSPF      0         0        0        0
ISIS      0         0        0        0
BGP       0         0        0        0
TOTAL     3         0        0        3

```

### Examples

The following example displays the statistics of all routing tables.

```

Hostname# show ip route summary all
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

IP routing table count: 0
Total
Memory: 13104 bytes
Entries: 6, based on route prefixes

```

```

                NORMAL    ECMP      FRR      TOTAL
Connected 4         0         0         4
Static    1         1         0         2
RIP       0         0         0         0
OSPF      0         0         0         0
ISIS      0         0         0         0
BGP       0         0         0         0
TOTAL     5         1         0         6

Global
Memory: 13104 bytes
Entries: 6, based on route prefixes

                NORMAL    ECMP      FRR      TOTAL
Connected 4         0         0         4
Static    1         1         0         2
RIP       0         0         0         0
OSPF      0         0         0         0
ISIS      0         0         0         0
BGP       0         0         0         0
TOTAL     5         1         0         6
    
```

Field	Description
NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

### 1.11 show ipv6 route

Use the command to display the configuration of the IPv6 routing table.

**show ipv6 route** [ [ *ipv6-prefix / prefix-length* [ **longer-prefixes** ] | *protocol* | **weight** ] ]

Parameter	Description
<i>ipv6-prefix/prefix-length</i>	(Optional) Specifies a prefix for route's IPv6 address.
<b>longer-prefixes</b>	(Optional) Displays the route with an IPv6 address prefix mostly matched.
<i>protocol</i>	((Optional) Displays the route information of specific protocol.
<i>process-id</i>	(Optional) Specifies a route process ID.
<b>weight</b>	(Optional) Displays the non-default-weight routes only.

**Defaults** N/A

**Command Mode** All CLI user modes except user EXEC mode

**Usage Guide** Use this command to display route information.

The following example displays the IPv6 routing table.

```

Hostname# show ipv6 route

IPv6 routing table - Default - 7 entries
Codes: C - Connected, L - Local, S - Static
       R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       IA - Inter area

C    10::/64 via Loopback 1, directly connected
L    10::1/128 via Loopback 1, local host
S    20::/64 [20/0] via 10::4, Loopback 1C
C    FE80::/10 via Null 0, directly connected
C    FE80::/64 via Loopback 1, directly connected
L    FE80::2D0:F8FF:FE22:33AB/128 via Loopback 1, local host
    
```

**Examples**

Field	Description
-------	-------------



C	Source routing protocol, which may be: C: directly connected route L: local host S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands	Command	Description
	<b>ipv6 route</b>	Configures the IPv6 static route.

**Platform** N/A  
**Description**

## 1.12 show ipv6 route summary

Use this command to display the statistics of the IPv6 routing table.

**show ipv6 route summary**

Use this command to display statistics of all IPv6 routing tables.

**show ipv6 route summary all**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command** All CLI user modes except user EXEC mode

**Mode**

**Usage Guide** N/A

The following example displays statistics of IPv6 global routing table.

```

Hostname# show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected     3
Static        0
-----
Total         5
    
```

**Examples**

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Local : Local host entry Connected: Connected route entry. Static: Static route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global TOTAL: All routing table summaries.

The following example displays the statistics of all IPv4 routing tables.

```

Hostname# show ipv6 route summary all

IPv6 routing table count: 1
Total
  Memory: 21840 bytes
  Entries: 10
    Local:4,Connected:5,Static:1,RIP:0,OSPF:0,ISIS:0,BGP:0

Global
  Memory: 21840 bytes
  Entries: 10
    Local:4,Connected:5,Static:1,RIP:0,OSPF:0,ISIS:0,BGP:0
    
```

Field	Description
Memory	The memory size occupied by the current routing table.

Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Local : Local host entry Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry. ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.
IPv6 routing table count	The number of the routing tables.
Global	The name of the current routing table. The field can be: Global : Global TOTAL: All routing table summaries.

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**



# Multicast Commands

---

1. IGMP Snooping Commands

# 1 IGMP Snooping Commands

## 1.1 clear ip igmp snooping gda-table

Use this command to clear the Group Destination Address (GDA) table.

**clear ip igmp snooping gda-table**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the <b>clear ip igmp snooping gda-table</b> command.	
<b>Configuration Examples</b>	The following example clears the Group Destination Address (GDA) table.	
	<pre>Hostname# clear ip igmp snooping gda-table</pre>	
<b>Platform Description</b>	N/A	

## 1.2 ip igmp snooping

Use this command to enable IGMP snooping.

**ip igmp snooping**

Use the **no** or **default** command to restore the default setting.

**no ip igmp snooping**

**default ip igmp snooping**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

**Defaults** IGMP snooping is disabled by default.

<b>Command</b>	Global configuration mode
<b>Mode</b>	
<b>Usage Guide</b>	<p><b>IVGL (Independent VLAN Group Learning):</b> In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.</p> <p>PIM snooping relies on the IVGL mode of IGMP snooping. Therefore, if the <b>no ip igmp snooping</b> command is executed to disable IGMP snooping when PIM snooping is implemented, the disabling fails and a message is displayed, indicating that PIM snooping must be disabled first.</p>
<b>Configuration</b>	The following example enables IGMP Snooping and enters the IVGL mode.
<b>Examples</b>	<pre>Hostname(config)# ip igmp snooping</pre>
<b>Platform</b>	N/A
<b>Description</b>	

### 1.3 ip igmp snooping fast-leave enable

Use this command to enable the fast leave function.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping fast-leave enable**

**no ip igmp snooping fast-leave enable**

**default ip igmp snooping fast-leave enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command**  
**Mode** Global configuration mode

**Usage Guide** After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message. Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets include IGMPv2 leave packets and IGMPv3 report packets of the include type without source addresses. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.

**Configuration** The following example enables the fast leave function.

**Examples**

```
Hostname(config)# ip igmp snooping fast-leave
```

**Platform** N/A

**Description**

## 1.4 ip igmp snooping host-aging-time

Use this command to configure the aging time of IGMP dynamic ports.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping host-aging-time** *seconds*

**no ip igmp snooping host-aging-time**

**default ip igmp snooping host-aging-time**

Parameter	Parameter	Description
<b>Description</b>	<i>seconds</i>	Aging time. The unit is second. The value ranges from 1 to 65,535.

**Defaults** The default is 260 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group.

When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by **host-aging-time**. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the **ip igmp snooping host-aging-time** command is executed, the aging time will be determined by **host-aging-time**. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.

**Configuration Examples** The following example sets the aging time to 30 seconds.

```
Hostname(config)# ip igmp snooping host-aging-time 30
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.5 ip igmp snooping ignore-query-timer

Use this command to ignore the query timer.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping ignore-query-timer**

**no ip igmp snooping ignore-query-timer**  
**default ip igmp snooping ignore-query-timer**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** The query timer is not ignored by default.

**Command  
Mode** Global configuration mode

**Usage Guide** This command is used for instable networks like WLAN, in case that the interface ages due to report packet loss.

**Configuration** The following example ignores the query timer.

**Examples** `Hostname(config)# ip igmp snooping ignore-query-timer`

**Platform** N/A

**Description**

## 1.6 ip igmp snooping mcast-to-unicast enable

Use this command to enable multicast-to-unicast forwarding.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping mcast-to-unicast enable**  
**no ip igmp snooping mcast-to-unicast enable**  
**default ip igmp snooping mcast-to-unicast enable**

**Parameter  
Description**


Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command  
Mode** Global configuration mode

**Usage Guide** In unicast WLAN, this function is supported only on APs.

- With this function enabled, packets arriving at APs are differentiated in whether to apply this function.

 This function takes effect only when enabled on users following multicast-to-unicast policies like the packet rate and the group range.



**Configuration** The following example enables multicast-to-unicast forwarding.

**Examples**

```
Hostname(config)# ip igmp snooping mcast-to-unicast enable
```

**Platform** N/A

**Description**

## 1.7 ip igmp snooping mcast-to-unicast group-range

Use this command to set the multicast-to-unicast group range.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping mcast-to-unicast group-range** *ip-address ip-address*

**no ip igmp snooping mcast-to-unicast group-range**

**default ip igmp snooping mcast-to-unicast group-range**

Parameter	Parameter	Description
Description	<i>ip-address</i>	The group range from 224.0.1.0 to 239.255.255.255

**Defaults** No multicast-to-unicast group range is set by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** In unicast WLAN, this function is supported only on APs.

This function optimizes bandwidth utilization, which only permits the multicast-to-unicast forwarding of groups in need.

**Configuration** The following example sets the multicast-to-unicast group range in the global configuration mode.

**Examples**

```
Hostname(config)# ip igmp snooping mcast-to-unicast group-range 239.1.1.1
239.10.1.1
```

**Platform** N/A

**Description**

## 1.8 ip igmp snooping mcast-to-unicast max-group

Use this command to set the maximum multicast-to-unicast group number.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping mcast-to-unicast max-group** *number*

**no ip igmp snooping mcast-to-unicast max-group**

**default ip igmp snooping mcast-to-unicast max-group**

<b>Parameter Description</b>	Parameter	Description
	<i>number</i>	The maximum group number from 1 to 64
<b>Defaults</b>	The default is 64.	
<b>Command Mode</b>	Fat AP: Global configuration mode	
<b>Usage Guide</b>	<p>In unicast WLAN, this function is supported only on APs.</p> <p>This function optimizes bandwidth utilization, which only permits the multicast-to-unicast forwarding of groups with the configured number. When the bandwidth is not enough, use this command to reduce the maximum group number. When a multicast group is deleted, this command allows another group to join in the activity.</p>	
<b>Configuration Examples</b>	The following example sets the maximum multicast-to-unicast group number in global configuration mode.	
	<pre>Hostname(config)# ip igmp snooping mcast-to-unicast max-group 10</pre>	
<b>Platform Description</b>	N/A	

## 1.9 ip igmp snooping querier

Use this command to enable the IGMP querier.

Use **no** or **default** form of this command to restore the default setting.

**ip igmp snooping [ vlan *vid* ] querier**

**no ip igmp snooping [ vlan *vid* ] querier**

**default ip igmp snooping [ vlan *vid* ] querier**

<b>Parameter Description</b>	Parameter	Description
	<i>vlan vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.
<b>Defaults</b>	This function is disabled by default.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	<p>After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.</p> <p>If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.</p>	

**Configuration** The following example enables the IGMP querier function in VLAN 1.

**Examples**

```

Hostname(config)# ip igmp snooping querier
Hostname(config)# ip igmp snooping vlan 1 querier

```

**Platform** N/A

**Description**

## 1.10 ip igmp snooping querier address

Use this command to specify a source IP address for IGMP querier.

Use **no** or **default** form of this command to remove the source IP address configured.

**ip igmp snooping [ vlan *vid* ] querier address *ip-address***

**no ip igmp snooping [ vlan *vid* ] querier address**

**default ip igmp snooping [ vlan *vid* ] querier address**

**Parameter  
Description**

Parameter	Description
<b>vlan <i>vid</i></b>	VLAN ID. By default, the specified version is supported on all VLANs.
<b><i>ip-address</i></b>	Source IP address of the IGMP querier

**Defaults** N/A

**Command  
Mode** Global configuration mode

**Usage Guide** After enabling IGMP querier, you must configure a source IP address for the IGMP querier to activate this function.  
If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.

**Configuration** The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device.

**Examples**

```

Hostname(config)# ip igmp snooping querier address 1.1.1.1

```

The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3.

```

Hostname(config)# ip igmp snooping vlan 3 querier address 1.1.1.1

```

**Platform**

**Description**

## 1.11 ip igmp snooping querier max-response-time

Use this command to configure the maximum response time of the IGMP querier.

Use **no** or **default** form of this command to restore to the default setting.

**ip igmp snooping [ vlan *vid* ] querier max-response-time *seconds***

**no ip igmp snooping [ vlan *vid* ] querier max-response-time**  
**default ip igmp snooping [ vlan *vid* ] querier max-response-time**

**Parameter  
Description**

Parameter	Description
<b>vlan <i>vid</i></b>	VLAN ID. By default, the specified version is supported on all VLANs.
<b><i>seconds</i></b>	Maximum response time from 1 to 25 in the unit of seconds

**Defaults** The default is 10 seconds.

**Command  
Mode** Global configuration mode

**Usage Guide** Configure this command to specify the maximum response time to query packets.  
 By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration** The following example specifies the maximum response time of the IGMP querier on the device.

**Examples** `Hostname(config)# ip igmp snooping querier max-response-time 15`

The following example specifies the maximum response time of the IGMP querier in VLAN 1.

`Hostname(config)# ip igmp snooping vlan 1 querier max-response-time 15`

**Platform** N/A

**Description**

## 1.12 ip igmp snooping querier query-interval

Use this command to specify the interval for IGMP querier to send query packets.

Use **no** or **default** form of this command to restore the default setting.

**ip igmp snooping querier query-interval *seconds***

**no ip igmp snooping querier query-interval**

**default ip igmp snooping [ vlan *vid* ] querier query-interval**

**Parameter  
Description**

Parameter	Description
<b><i>seconds</i></b>	Query interval from 1 to 18,000 in the unit of seconds
<b>vlan <i>vid</i></b>	VLAN ID. By default, the specified version is supported on all VLANs.

**Defaults** The default is 60 seconds.

**Command  
Mode** Global configuration mode

**Usage Guide** If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration** The following example configures the query interval on the device.

**Examples**

```
Hostname(config)# ip igmp snooping querier query-interval 100
```

The following example configures the query interval in VLAN 1.

```
Hostname(config)# ip igmp snooping vlan 1 querier query-interval 100
```

**Platform** N/A

**Description**

## 1.13 ip igmp snooping querier timer expiry

Use this command to specify the expiration timer for non-querier.

Use **no** form of this command to restore the default setting.

**ip igmp snooping [ vlan vid ] querier timer expiry seconds**

**no ip igmp snooping [ vlan vid ] querier timer expiry seconds**

**default ip igmp snooping [ vlan vid ] querier timer expiry**

Parameter Description	Parameter	Description
	<i>seconds</i>	The expiration timer from 60 to 300 in the unit of seconds
	<b>vlan vid</b>	VLAN ID. By default, the specified version is supported on all VLANs.

**Defaults** The default is 125 seconds.

**Command Mode** Global configuration mode

**Usage Guide** After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier.

If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.

**Configuration** The following example configures the non-querier expiration timer on the device.

**Examples**

```
Hostname(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
Hostname(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

**Platform** N/A

**Description**

## 1.14 ip igmp snooping querier version

Use the following commands to specify IGMP Snooping querier version.

**ip igmp snooping [ vlan *vid* ] querier version 1**

**ip igmp snooping [ vlan *vid* ] querier version 2**

Use **no** or **default** form of this command to restore to the default setting.

**no ip igmp snooping [ vlan *vid* ] querier version**

**default ip igmp snooping [ vlan *vid* ] querier version**

<b>Parameter Description</b>	Parameter	Description
	<b>vlan <i>vid</i></b>	VLAN ID. By default, the specified version is supported on all VLANs.
<b>Defaults</b>	The default version is IGMPv2.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.	
<b>Configuration Examples</b>	The following example configures IGMP querier version on the device.	
	<pre>Hostname(config)# ip igmp snooping querier version 1</pre>	
<b>Platform Description</b>	N/A	

## 1.15 ip igmp snooping query-max-response-time

Use this command to specify the time for the switch to wait for the member join message after receiving the **query** message.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping query-max-response-time *seconds***

**no ip igmp snooping query-max-resposne-time**

**default ip igmp snooping query-max-response-time**

<b>Parameter Description</b>	Parameter	Description
	<b><i>seconds</i></b>	The aging time of the routing interface that the switch learns dynamically, in the range from 1 to 65.535

**Defaults** The default is 10 seconds.

<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	<p>You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member.</p> <p>This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.</p>
<b>Configuration Examples</b>	<p>The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.</p> <pre>Hostname(config)# ip igmp snooping query-max-response-time 100</pre>
<b>Platform Description</b>	N/A

## 1.16 ip igmp snooping suppression enable

Use this command to enable IGMP snooping suppression.

Use the **no** or **default** form of this command to restore the default setting.

**ip igmp snooping suppression enable**

**no ip igmp snooping suppression enable**

**default ip igmp snooping suppression enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks.

This function is only supported on IGMPv1 and IGMPv2 reports.

**Configuration Examples** The following example enables IGMP snooping suppression on the device.

```
Hostname(config)# ip igmp snooping suppression enable
```

**Platform Description** N/A

## 1.17 ip igmp snooping vlan

Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode.


Use the **no** form of this command is used to disable the IGMP Snooping.

Use the **default** form of this command to restore the default setting.

**ip igmp snooping vlan** *vid*

**no ip igmp snooping vlan** *vid*

**default ip igmp snooping vlan** *vid*

<b>Parameter Description</b>	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
<b>Defaults</b>	IGMP Snooping is disabled by default.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	Use this command to enable or disable the IGMP snooping on the specified vlan.	
	 The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.	
<b>Configuration Examples</b>	The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 1.	
	<pre> Hostname(config)# ip igmp snooping Hostname(config)# no ip igmp snooping vlan 1           </pre>	
<b>Platform Description</b>	N/A	

## 1.18 ip igmp snooping vlan fast-leave enable

Use this command to enable fast-leave function for the specified VLAN.

Use the **no** form of this command to disable this function.

Use the **default** form of this command to restore the default setting.

**ip igmp snooping vlan** *vid* **fast-leave enable**

**no ip igmp snooping vlan** *vid* **fast-leave enable**

**default ip igmp snooping vlan** *vid* **fast-leave enable**

<b>Parameter Description</b>	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094



<b>Defaults</b>	This function is enabled by default.
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	This command must be used with the <b>ip igmp snooping fast-leave enable</b> command.
<b>Configuration</b>	The following example disables the fast-leave function for VLAN 1.
<b>Examples</b>	<pre>Hostname(config)# no ip igmp snooping vlan 1 fast-leave enable</pre>
<b>Platform</b>	N/A
<b>Description</b>	

## 1.19 ip igmp snooping vlan mrouter interface

Use this command to configure a static routing interface.

Use the **no** form of this command to delete a static routing interface.

Use the **default** form of this command to restore the default setting.

**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*

**no ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*

**default ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
	<i>interface-type</i> <i>interface-number</i>	Interface ID

<b>Defaults</b>	No static routing interface is configured by default.
<b>Command Mode</b>	Global configuration mode
<b>Usage Guide</b>	<p>A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.</p> <p>When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded.</p> <p>When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.</p>
<b>Configuration</b>	The following example configures a static routing interface.
<b>Examples</b>	<pre>Hostname(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/1</pre>

**Platform** N/A

**Description**

## 1.20 ip igmp snooping vlan static interface

Use this command to configure a static member interface of a multicast group.

Use the **no** form of this command to delete a static member interface from a multicast group.

Use the **default** form of this command to restore the default setting.

**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type* *interface-number*

**no ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type* *interface-number*

**default ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type* *interface-number*

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
	<i>ip-addr</i>	Multicast IP address
	<i>interface-id</i>	Interface ID

**Defaults** No static member interface of any multicast group is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the **clear ip igmp snooping gda-table** command.

**Configuration Examples** The following example configures a static member interface for the multicast group 224.1.1.1.

```
Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
gigabitethernet 0/1
```

**Platform** N/A

**Description**

## 1.21 ip multicast wlan

Use this command to enable global multicast mode.

Use the **no** or **default** form of this command to restore the default setting.

**ip multicast wlan**

**no ip multicast wlan**

**default ip multicast wlan**

Parameter Description	Parameter	Description
	N/A	N/A
<b>Defaults</b>	Global multicast mode is disabled by default.	
<b>Command Mode</b>	Global configuration mode	
<b>Usage Guide</b>	With global multicast mode disabled, APs will discards received multicast packets without disposals.	
<b>Configuration Examples</b>	The following example enables global multicast mode.	
	<pre>Hostname(config)# ip multicast wlan</pre>	
<b>Platform Description</b>	N/A	

## 1.22 show ip igmp snooping

Use this command to display related information of IGMP Snooping.

**show ip igmp snooping** [*gda-table* / *mrouter* | *querier* [ *detail* | *vlan vid* ] / *user-info* | *vlan vid*]

Parameter Description	Parameter	Description
	<i>vlan vid</i>	VLAN ID. By default, IGMP Snooping querier information of all VLANs are displayed.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example displays global IGMP Snooping information.	
	<pre>Hostname#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable</pre>	

```
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

The following example displays VLAN1 IGMP Snooping information.

```
Hostname#show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Response Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-----
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disable
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

**Platform** N/A  
**Description**

## 1.23 show ip multicast wlan

Use this command to display global WLAN multicast configuration.

**show ip multicast wlan**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** Use this command to check whether global WLAN multicast configuration is enabled.

**Configuration Examples** The following example displays global WLAN multicast configuration.

```
Hostname#show ip multicast wlan
Global multicast state: enable
```

**Platform**      N/A  
**Description**



# AP Management Commands

---

1. CAPWAP Commands
2. iBeacon Commands

# 1 CAPWAP Commands

## 1.1 acip ipv4

Use this command to configure the AP to join a specified AC. Use the **no** form of this command to remove the configuration.

**acip ipv4** *ip-address* [*ip-address...*]

**no acip ipv4**


Parameter	Description
<i>ipv4-address</i>	Indicates the static IP address. Up to six static addresses can be configured.

**Defaults** N/A

**Command Mode** AP global configuration mode

### Usage Guide

In general, the fit AP has no configuration. You can find AC through broadcast, multicast, DHCP and DNS or joining AC through the AC address configured by the static address. AP sends a discovery request packet to these IP addresses to detect whether AC is valid, and then add an AC.

 If this command is configured for the fit AP and the AC connected with it, then the final configuration is the AC configuration.

### Configuration Examples

The following example configures the static IP address list for the fit AP to join AC as 192.168.1.1 and 192.168.2.1.

```
Hostname(config)# acip ipv4 192.168.1.1 192.168.2.1
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 acip ipv6

Use this command to configure an AP to join an AC with a specific IPv6 address. Use the **no** form of this command to remove the configuration.

**acip ipv6** *ipv6-address* [*ipv6-address...*]

**no acip ipv6**


Parameter	Description
<i>ipv6-address</i> &<1~6>	Specifies the IPv6 address of the AC to be connected with the AP. Up to six static addresses can be configured.

**Defaults** N/A

**Command Mode** AP global configuration mode/AP configuration mode on the AC

An AP can find ACs through IPv6 multicast, DHCPv6, or DNSv6 packets or join an AC with a specific static IPv6 address. After this command is configured, the AP sends discovery request packets to the static IPv6 address of the AC to detect whether the address is valid. If the address is valid, the AP will join the AC.

**Usage Guide**

 If this command is configured on a fit AP and an AC connected with the AP, only the configuration on the AC takes effect.

The following example configures a fit AP to join an AC with static IPv6 address 2001:1a2b::1234.

```
Hostname(config)# acip ipv6 2001:1a2b::1234
```

**Configuration Examples**

The following example configures AP0001 to join an AC with static IPv6 address 2001:1a2b::1234.

```
Hostname(config)# ap-config AP0001
```

```
Hostname(config-ap)# acip ipv6 2001:1a2b::1234
```

Command	Description
<b>acip ipv4</b>	Specifies the IPv4 address of an AC to be connected with the AP.

**Related Commands**

**Platform Description** N/A




### 1.3 apip ipv4

Use this command to configure a static IP address for a specified AP. Use the **no** form of the command to remove the configuration.

**apip ipv4** *ipv4-address network-mask gateway*

**no apip ipv4**



	Parameter	Description				
<b>Parameter</b>	<i>ipv4-address</i>	The static IPv4 address.				
<b>Description</b>	<i>network-mask</i>	The subnet mask.				
	<i>gateway</i>	The gateway address.				
<b>Defaults</b>	N/A					
<b>Command Mode</b>	AP global configuration mode					
	<p>In general, the fit AP has no configuration. Its IP address and gateway can be dynamically obtained by DHCP. When the CAPWAP tunnel between AP and AC is established, AC delivers the static IP address for AP, so that the address of AP maintains unchanged after AP is rebooted. In special application scenario, you can configure this command in AP global configuration mode to manually set the static IP address for the fit AP.</p>					
<b>Usage Guide</b>	<p> 1. With the AP address configured as static, the DHCP is disabled, and the AC address cannot be obtained through the OPTION of DHCP. Therefore, after this command is configured, you need to configure the AC address using the <b>acip ipv4</b> command on the AP so that the AP can find and join the AC when the AP and the AC are not in the same subnet.</p> <p> 2. The configuration of this command will be automatically saved after the AP configuration. No command of saving is required to be executed.</p> <p> 3. This command serves the same purpose as the <b>ip address</b> command on the AC in the AP configuration mode. However, when the AP joins the AC, if the <b>ip address</b> command exists in the AP configuration mode of the AC and conflicts with the <b>apip ipv4</b> command, the static address of the AP will be updated and the CAPWAP tunnel will be re-created.</p>					
<b>Configuration Examples</b>	<p>The following example configures the static IP address of the fit AP as 192.168.1.2, the subnet mask as 255.255.255.0, and the gateway as 192.168.1.1.</p> <pre> Hostname(config)# apip ipv4 192.168.1.2 255.255.255.0 192.168.1.1 </pre>					
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>acip ipv4</b></td> <td>Specifies the AC address to be connected with by an AP.</td> </tr> </tbody> </table>	Command	Description	<b>acip ipv4</b>	Specifies the AC address to be connected with by an AP.	
Command	Description					
<b>acip ipv4</b>	Specifies the AC address to be connected with by an AP.					
<b>Platform Description</b>	N/A					

## 1.4 apip ipv4 enable

Use this command to enable IPv4 support on a specific AP. Use the **no** form of this command to remove the configuration.

**apip ipv4 enable**

**no apip ipv4 enable**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** IPv4 support is enabled on the AP by default.

**Command Mode** AP global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables IPv4 support on the fit AP.

```
Hostname(config)# no apip ipv4 enable
```

**Platform Description** N/A

## 1.5 apip ipv6

Use this command to configure a static IPv6 address for a specified AP. Use the **no** form of the command to remove the configuration.

**apip ipv6** *ipv6-address/prefix-length gateway*


**no apip ipv6**



Parameter	Parameter	Description
Description	<i>ipv6-address/prefix-length</i>	The IPv6 address with the mask length, for example. X:X:X::X/24.
	<i>gateway</i>	Gateway address.

**Defaults** N/A

**Command Mode** AP global configuration mode

**Usage Guide** This command is used to configure a static IPv6 address for the AP.

-  1. With the AP IPv6 address configured as static, the DHCPv6 is disabled, and the AC address cannot be obtained through the OPTION of DHCPv6. Therefore, after this command is configured, you need to configure the AC IPv6 address using the **acip ipv6** command on the AP and enable IPv6 support for the AP using the **apip ipv6 enable** command so that the AP can find and join the IPv6 AC when the AP and the AC are not in the same subnet.

-  2. The configuration of this command will be automatically saved.
-  3. This command serves the same purpose as the **ipv6 address** command on the AC in the AP configuration mode. However, when the AP joins the AC, the **ipv6 address** command in the AP configuration mode on the AC will conflict with the **apip ipv6** command, the static IPv6 address of the AP will be updated and the CAPWAP tunnel will be re-created.

**Configuration Examples** The following example configures the static IPv6 address of the fit AP as 2001:1a2b:1234::5566/48, and the gateway as 2001:1a2b:1234::1.

```
Hostname (config) # apip ipv6 address 2001:1a2b:1234::5566/48 2001:1a2b:1234::1
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.6 apip ipv6 address autoconfig default

Use this command to configure an AP to obtain a static IPv6 address through the automatic IPv6 address configuration mechanism. Use the **no** form of this command to remove the configuration.

- apip ipv6 address autoconfig default**
- no apip ipv6 address autoconfig default**


**Parameter Description**

Parameter	Description
N/A	N/A



**Defaults** N/A

**Command Mode** AP global configuration mode

**Usage Guide** You can run this command to configure a static IPv6 address for the AP. The configuration is similar to static IPv4 address configuration by running the **apip** command.

-  1. If a static IPv6 address is set for the AP, DHCPv6 will be disabled. As a result, the AP cannot obtain IPv6 addresses of ACs through DHCPv6 OPTION. Therefore, after running this command, you must run the **acip ipv6** command to specify an IPv6 address of an AC to be connected with

the AP, and use the **apip ipv6 enable** command to enable IPv6 support on the AP. After this configuration, the AP can discover and join the AC even if they are not on the same sub-network.

-  2. When this command is run on the AP, the configuration is saved automatically instead of being saved by running the configuration saving command.
-  3. This command has the same function as the **ipv6 address** command used on an AC in AP configuration mode. Configuring this command does not affect configuration of the AC. When the AP joins the AC, if the **ipv6 address** command is run on the AC in AP configuration mode and conflicts with the **apip ipv6** command, the AP will update its static IPv6 address and re-establish CAPWAP tunnels.

**Configuration Examples** The following example configures an AP to obtain a static IPv6 address through the automatic IPv6 address configuration mechanism.

```
Hostname(config)# apip ipv6 autoconfig default
```

**Platform** N/A  
**Description**

## 1.7 apip ipv6 enable

Use this command to enable IPv6 support on a specific AP. Use the **no** form of this command to remove the configuration.

- apip ipv6 enable**
- no apip ipv6 enable**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** IPv6 support is enabled on the AP by default.

**Command Mode** AP global configuration mode

You can run this command to enable IPv6 support or run the **no** form of this command to disable IPv6 support. If an AP enabled with IPv6 support has no static IPv6 address, it will dynamically obtain an IPv6 address through DHCPv6. If IPv6 support is disabled from the AP, DHCPv6 is also disabled, but configuration about the static IPv6 address is not deleted.

- Usage Guide**
1. If the IPv6 support state of the AP is changed, the AP will re-establish CAPWAP tunnels.
  2. IPv6 support configuration of the AP is saved in a flash memory and remains unchanged when the AP is restarted.

The following example enables IPv6 support on the fit AP.

**Configuration** `Hostname(config)# apip ipv6 enable`

The following example disables IPv6 support from the fit AP.

**Examples** `Hostname(config)# no apip ipv6 enable`

Command	Description
<b>apip ipv6 address</b>	Specifies the IPv6 address of the AC to be connected with the AP.
<b>ipv6 enable</b>	Enables IPv6 support on the specific AP on the AC in AP configuration mode.

**Platform** N/A

**Description**

## 1.8 apip pppoe

Use this command to enable the AP to obtain the address through PPPoE. Use the **no** form of this command to restore the default setting.

**apip pppoe**  
**no apip pppoe**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** AP global configuration mode

**Usage Guide** After configuring this command, you should perform PPPoE and configure the default route to point to the dialer interface to enable communication between the AP and the AC.

 CAPWAP can select only dialer 1 as the source port. Therefore, PPPoE dial requires dialer 1.

**Configuration** The following example enables the fit AP to obtain the address through PPPoE.

**Examples** `Hostname(config)# apip pppoe`

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.9 ap-mode

Use these commands to switch AP to fit mode or to fat mode.

**ap-mode** { fit | fat [ dhcp ] | macc }

Parameter	Description
<b>fit</b>	Switches the AP to fit mode.
<b>fat</b>	Switches the AP to fat mode.
<b>dhcp</b>	When this parameter is configured, the AP enables DHCP to obtain IP address by default; Otherwise the AP uses static IP addresses by default.
<b>macc</b>	Switches the AP to MACC mode.

**Defaults** The default AP mode is MACC.



**Command Mode** Global configuration mode

After switching the AP working mode, restart the device to ensure the configuration consistency.

When working as a fat AP, the default IP address of the rear end wired interface (Which is connected to the PoE switching device) is 192.168.110.1/255.255.255.0; the default IP address of the front end wired interface (the Ethernet port on the front panel) is 192.168.111.1/255.255.255.0.

When the command **ap-mode fat dhcp** is configured, once the AP is switched to fat mode, the fat AP will obtain IP address through DHCP. After AP is restarted without further related configuration, it will still obtain IP address through DHCP.

### Usage Guide

-  When the command **ap-mode fat dhcp** is configured on the WALL-AP, DHCP is enabled only on the rear end wired interface by default; that is to say, by default, the front end interface still uses static IP address.
-  You cannot use commands **ap-mode fat dhcp** and **ap-mode fat** to perform direct switchover in the fat mode. You should switch to fit mode and then perform such switchover.

**Configuration Examples** The following example switches the AP to fit mode:

```
Ruijie(config)# ap-mode fit
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** The command is supported only on APs.

## 1.10 show ap-mode

Use this command to display the AP mode.

**show ap-mode**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the AP mode.

**Examples**

```
Ruijie# show ap-mode
current mode: MACC
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description**

## 1.11 show capwap detail

Use this command to display details about the CAPWAP tunnel.

**show capwap { index | ip-address [ port ] } detail**

Parameter Description	Parameter	Description
	<i>index</i>	Tunnel index.
	<i>ip-address</i>	Tunnel IP address.
	<i>port</i>	Tunnel port number.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays details about the CAPWAP tunnel whose address is 1.1.1.1.

**Examples**

```

Hostname# show capwap 1.1.1.1 detail
CAPWAP process "capwap 1" with state Run
  Process uptime is 3 days 0 hour 41 minutes
  Echo interval is 30 secs, Dead interval is 81 secs
  Current timers echo-interval
  Peer address is 172.18.59.5
  Peer control port is 10000, data port is 10001
  My address is 55.55.55.60
  The MAC of AP is 001a.a94e.d773
  The Session ID of AP is 001a.a94e.d773.53e1.0801.53e1.0801.53e1
  The Path MTU is 1500
  Recent received request's sequence number 39
  Recent received response's sequence number 11
  Recent send request's sequence number 11
  Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0
  Sending queue length 0, Receive queue length 0
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.12 show capwap state

Use this command to display the CAPWAP tunnel state.

**show capwap state**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode



**Usage Guide** N/A

**Configuration** The following example displays the CAPWAP tunnel state.

**Examples**

```

Hostname#show capwap state
CAPWAP tunnel state, 3 peers, 2 is run:
Index Peer IP Peer Port State Mac Address
1 192.168.0.1 10000 Run 001a.a900.0001
2 192.168.0.2 10000 Run 001a.a900.0002
3 192.168.0.3 10000 DTLS Teardown 001a.a900.0003
    
```

Field	Description
Index	Tunnel index.
Peer IP	Peer IP address.
Peer Port	Peer port number.
State	Tunnel state.
Mac Address	AP MAC address, only displayed on ACs.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 1.13 show capwap statistics

Use this command to display statistics about the CAPWAP tunnel packets.

**show capwap { index | ip-address [ port ] } statistics**

Parameter Description	Parameter	Description
	index	Tunnel index.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays packet statistics about the CAPWAP tunnel whose IP address is 1.1.1.1.

```

Hostname#show capwap 1.1.1.1 statistics
    
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description**

N/A

# 1 iBeacon Commands

## 1.1 ibeacon uuid major minor

Use this command to configure the iBeacon function for the specified AP.

**ibeacon uuid** *uuid major major minor minor*

Use the **no** form of this command to disable the iBeacon function of an AP.

**no ibeacon**

Parameter Description	Parameter	Description
	<i>uuid</i>	The value of <b>uuid</b> is a string consisting of 32 hexadecimal characters.
	<i>major</i>	The value of <b>major</b> is a string consisting of four hexadecimal characters.
	<i>minor</i>	The value of <b>minor</b> is a string consisting of four hexadecimal characters.

**Defaults** iBeacon is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure the iBeacon function for an AP.  
The configuration takes effect on only the APs supporting Bluetooth.

**Configuration Examples** 1: The following example configures the iBeacon function directly on an AP.

```
Hostname(config)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154
```

2: The following example disables the iBeacon function of an AP.

```
Hostname(config)# no ibeacon
```

**Verification** 1: Run the **show running** command on an AP device to display iBeacon parameters.

**Displayed Message** -

**Common Errors** N/A

**Platform Description** N/A

## 1.2 ibeacon uuid major minor radio

Use this command to configure the iBeacon function based on BT Radio for the specified AP.

**ibeacon uuid** *uuid major major minor minor radio radio-id*

Use the **no** form of this command to disable the iBeacon function based on BT Radio.

**no ibeacon radio** *radio-id*

Parameter Description	Parameter	Description
	<i>uuid</i>	The value of <b>uuid</b> is a string consisting of 32 hexadecimal characters.
	<i>major</i>	The value of <b>major</b> is a string consisting of four hexadecimal characters.
	<i>minor</i>	The value of <b>minor</b> is a string consisting of four hexadecimal characters.
	<i>radio-id</i>	The value is an integer in the range from 1 to 255. The number of supported radios varies with different products.

**Defaults** BT-Radio-based iBeacon function is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure the iBeacon function based on BT radio. The configuration takes effect on only the APs supporting Bluetooth.

**Configuration Examples** The following example configures the iBeacon function based on BT Radio on an AP.

```
Hostname(config)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 radio 1
```

The following example disables the iBeacon function based on BT Radio.

```
Hostname(config)# no ibeacon radio 1
```

**Verification** 1: Run the **show running** command on an AP device to display BT-Radio-based iBeacon parameters.

**Displayed Message** -

**Common Errors** N/A

**Platform Description** N/A



# STA Management Commands

---

1. FAT AP Commands
2. STA Management Commands

# Fat AP Commands

## 1.1 11acsupport enable

Use this command to enable the device to support 802.11ac. Use the **no** form of this command to disable 802.11ac.

**11acsupport enable**  
**no 11acsupport enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** When an RF interface provides the 802.11ac capability, 802.11ac STA access is supported by default.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example enables the device to support 802.11ac.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# 11acsupport enable

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.2 11asupport enable

Use the command to enable the device to support 802.11a. Use the **no** form of this command to disable 802.11a.

**11asupport enable**  
**no 11asupport enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** 802.11a STA access is supported.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example enables the device to support 802.11a.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# llasupport enable

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.3 11ax-gi

Use this command to configure 11ax-gi for the specified radio. Use the **no** form of this command to restore the default settings.

**11ax-gi { 0.8 | 1.6 | 3.2 | auto }**  
**no 11ax-gi**

Parameter Description	Parameter	Description
	<b>0.8</b>	Sets 11ax-gi to 0.8us.
<b>1.6</b>	Sets 11ax-gi to 1.6us.	
<b>3.2</b>	Sets 11ax-gi to 3.2us.	
<b>auto</b>	Sets 11ax-gi to auto.	

**Defaults** The default 11ax-gi is auto.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets 11ax-gi to 0.8us for radio 1.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# 11ax-gi 0.8

```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.4 11axsupport enable

Use this command to enable the device to support 802.11ax. Use the **no** form of this command to disable 802.11ax.

**11axsupport enable**  
**no 11axsupport enable**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** When an RF interface provides the 802.11ax capability, 802.11ax is disabled by default.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables the device to support 802.11ax.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# 11axsupport enable
    
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.5 11bsupport enable

Use the command to enable the specified radio to support 802.11b on 2.4 GHz. Use the **no** form of this command to disable the radio to support 802.11b on 2.4 GHz.

**11bsupport enable**  
**no 11bsupport enable**

<b>Parameter</b>	Parameter	Description



<b>Description</b>		
	-	-

**Defaults** By default, 802.11b is supported.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** The configuration is effective only when the RF interfaces of an AP operate at the 2.4 GHz band.

**Configuration Examples** The following example enables radio1 to support 802.11b on 2.4 GHz.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# no 11bsupport enable

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Platform Description** N/A

## 1.6 11gsupport enable

Use this command to enable the device to support 802.11g. Use the **no** form of this command to disable 802.11g.

**11gsupport enable**  
**no 11gsupport enable**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

**Defaults** 11g STA access is supported.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables the device to support 802.11g.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# no 11gsupport enable

```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 1.7 11n support enable

Use this command to enable the device to support 802.11n. Use the **no** form of this command to disable 802.11n.

**11n support enable**  
**no 11n support enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** 11n STA access is supported by default.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** This command is used to allow 802.11n STAs access.

**Configuration Examples** The following example enables the device to support 802.11n.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# 11n support enable

```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

## 1.8 ampdu

Use this command to enable a specified radio to support A-MPDU. Use the **no** form of this command to disable the radio to support A-MPDU.

**ampdu enable**  
**no ampdu enable**

Parameter Description	Parameter	Description

N/A	N/A
-----	-----

**Defaults** The A-MPDU aggregation mode is enabled.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** This command takes effect only when the radio operates in 802.11n.

**Configuration Examples** The following example enables radio1 to support A-MPDU.

```

Hostname(config)# interface dot11radio 1/0
Ruijie (config-if-Dot11radio 1/0)# ampdu enable

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.9 ampdu-depth

Use this command to configure the A-MPDU aggregation depth. Use the **no** or **default** form of this command to restore the default setting.

**ampdu-depth** *depth*

**no ampdu-depth**

**default ampdu-depth**

**Parameter Description**

Parameter	Description
<i>depth</i>	Configures the A-MPDU aggregation depth, in the range from 1 to 64.

**Defaults** No A-MPDU aggregation depth is configured by default.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** This command takes effect only when the radio operates in 802.11n, 802.11ac, or 802.11ax.

**Configuration Examples** The following example sets the A-MPDU aggregation depth to 12.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# ampdu-depth 12

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.10 ampdu-retries

Use this command to configure number of A-MPDU software re-transmission times.

**ampdu-retries** *times*

Parameter Description	Parameter	Description
	<i>times</i>	

**Defaults** The default value is 4.

**Command Mode** Dot11radio interface configuration mode.

**Usage Guide** The configuration is effective only when the RF interfaces operate at the 11n mode.

**Configuration Examples** The following example sets the A-MPDU software retransmission times to 2.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# ampdu-retries 2

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.11 ampdu-rts

Use this command to enable the Request to Send (RTS) protection mode for the A-MPDU packets.

Use the **no** form of this command to disable the RTS mode.

**ampdu-rts**

**no ampdu-rts**

Parameter Description	Parameter	Description

N/A	N/A
-----	-----

**Defaults** RTS protection is disabled by default.

**Command Mode** Dot11radio interface configuration mode.

**Usage Guide** The configuration is effective only when the RF interfaces operate at the 11n mode.

**Configuration Examples** The following example enables the A-MPDU RTS protection.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# ampdu-rts

```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.12amsdu

Use this command to enable or disable the A-MSDU aggregation mode.

**amsdu { enable | disable }**

**Parameter Description**

Parameter	Description
<b>enable</b>	Enables the A-MSDU aggregation mode.
<b>disable</b>	Disables the A-MSDU aggregation mode.

**Defaults** The A-MSDU aggregation mode is enabled by default.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** Enable A-MSDU to aggregate multiple MSDU into one MSDU. Through aggregation, A-MSDU reduces additional information for transmitting the MAC header, improving transmission efficiency on the MAC layer. With less frames, conflict is less likely to occur.

**Configuration Examples** The following example enables the A-MSDU aggregation mode on dot11radio 1/0.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# amsdu enable

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.13 antenna receive

Use this command to configure the receive mode of an antenna.

**antenna receive** *chain-mask*

Parameter Description	Parameter	Description
	<i>chain-mask</i>	

**Defaults** The quantity of antennas and the default antenna selection mask vary with product models.

**Command Mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the receive mode of the antenna to 2.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# antenna receive 2

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.14 antenna transmit

Use this command to configure the transmit mode of an antenna.

**antenna transmit** *chain-mask*

Parameter Description	Parameter	Description
	<i>chain-mask</i>	

**Defaults** The quantity of antennas and the default antenna mask vary with product models.

**Command** Dot11radio interface configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the transmit mode of the antenna to 2.

**Examples**

```
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# antenna transmit 2
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.15 antenna type

Use this command to configure an omnidirectional antenna or a directional antenna for a specified radio of a specified AP or of all APs in a specified AP group.

Use the **no** form of this command to configure the default antenna type for a specified radio of a specified AP or of all APs in a specified AP group.

Use the **default** form of this command to restore the default antenna type for a specified radio of a specified AP or of all APs in a specified AP group.

**antenna type { omnidirection | direction }**

**no antenna type**

**default antenna type**

**Parameter  
Description**

Parameter	Description
<b>omnidirection</b>	Indicates an omnidirectional antenna.
<b>direction</b>	Indicates a directional antenna.

**Defaults** An omnidirectional antenna is used by default.

**Command** dot11radio interface configuration mode

**Mode**

**Default Level** 14

**Usage Guide** 1: If omnidirectional or directional antennas need to be configured for all radios, perform configuration in interface range dot11radio configuration mode.

2: This command is applicable only to radios that support both omnidirectional and directional antennas.

3: If the internal antenna and external antenna can be switched, validate the configuration of internal and external antennas prior to that of omnidirectional and directional antennas.

**Configuration** The following example enables radio 1 to use a directional antenna.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# antenna type direction

```

**Verification** Run the **show running-config** command to display the transmit antenna configuration.

**Platform**  
**Description** N/A.

## 1.16apsd

Use this command to configure the unscheduled-automatic power save delivery (U-APSD) mode.

**apsd { enable | disable }**

Parameter Description	Parameter	Description
	<b>enable</b>	Enables the U-APSD mode.
	<b>disable</b>	Disables the U-APSD mode.

**Defaults** APSD mode is enabled by default.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example enables the U-APSD mode.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# apsd disable

```

Related Commands	Command	Description
	N/A	N/A

**Platform**  
**Description** N/A

## 1.17assoc-rssi

Use this command to configure the minimum RSSI that keeps STA access. Use the **no** form of this command to restore the default setting.

**assoc-rssi rssi-value**



**no assoc-rssi**

Parameter Description	Parameter	Description
	<i>rssi-value</i>	Indicates the minimum RSSI that keeps STA access. The range is from 0 to 100. The unit is dBm.

**Defaults** The minimum RSSI that keeps STA access is 0, which indicates that the access of all STAs is kept regardless of their RSSI values.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the minimum RSSI that keeps STA access to 15.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# assoc-rssi 15

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.18 autowifi

Use this command to enable the one-click WLAN configuration for an unconfigured device. Use the **no** form of this command to disable the one-click WLAN configuration.

**autowifi**

**no autowifi**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** The one-key WLAN configuration function is provided to implement rapid configuration for an empty device.

This function helps geological prospecting personnel to achieve rapid configuration and improve the operation efficiency, and helps channels to rapidly configure WLANs for performance testing.

**Configuration** The following example configures one-click WLAN configuration.

**Examples** `Hostname(config)# autowifi`

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.19 beacon dtim-period

Use this command to configure the period of delivery transmission indication messages (DTIM) for the specified radio. Use the **no** form of this command to restore the default setting.

**beacon dtim-period** *period-num*

**no beacon dtim-period**

**Parameter  
Description**

Parameter	Description
<i>period-num</i>	DTIM period. The range is from 1 to 255.

**Defaults** The DTIM period is at the interval of one beacon frame period.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the DTIM period to 30 beacon periods.

**Examples** `Hostname(config)# interface dot11radio 1/0`  
`Ruijie (config-if-Dot11radio 1/0)# beacon dtim-period 30`

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.20 beacon period

Use this command to configure the beacon frame period for the specified radio.

<b>beacon period</b> <i>milliseconds</i>					
<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>milliseconds</i></td> <td>Beacon period. The range is from 20 to 1,000. The unit is millisecond.</td> </tr> </tbody> </table>	Parameter	Description	<i>milliseconds</i>	Beacon period. The range is from 20 to 1,000. The unit is millisecond.
Parameter	Description				
<i>milliseconds</i>	Beacon period. The range is from 20 to 1,000. The unit is millisecond.				
<b>Defaults</b>	The default is beacon period is 100 milliseconds.				
<b>Command mode</b>	Dot11radio interface configuration mode.				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	The following example configures the beacon frame period to 200 milliseconds.				
	<pre> Hostname(config)# interface dot11radio 1/0 Hostname(config-if-Dot11radio 1/0)# beacon period 200 </pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
<b>Platform Description</b>	N/A				

## 1.21 beacon rate

Use this command to configure the beacon rate for the specified radio. Use the **no** form of this command to restore the default beacon rate.

**beacon rate** *beacon-rate*  
**no beacon**

<b>Parameter Description</b>	Parameter	Description
	<i>beacon-rate</i>	Specifies the beacon rate.
<b>Defaults</b>	No beacon rate is configured by default.	
<b>Command mode</b>	Dot11radio interface configuration mode.	
<b>Usage Guide</b>	<ul style="list-style-type: none"> <li>■ Do not configure a beacon frame transmission rate that is disabled in the data rate set settings.</li> <li>■ Because the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps rates are not supported in 5 GHz, do not set the beacon frame transmission rate to any of the preceding values for the radios in 5 GHz.</li> </ul>	

- If you select **802.11b**, the beacon frame transmission rate is configured for all the radios in 2.4 GHz. The settings take effect when the APs go online for the first time and are automatically applied to the radios. If you select **802.11a**, the condition is the same for the radios in 5.8 GHz.

**Configuration** The following example configures the beacon rate of radio1 to 12Mbps.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# beacon rate 12.0
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.22broadcast-ssid

Use the **broadcast-ssid** to broadcast SSIDs. Use the **no** form of this command to hide SSIDs.

- broadcast-ssid**
- no broadcast-ssid**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** SSIDs are broadcasted.

**Command mode** WLAN configuration mode

**Usage Guide** N/A

**Configuration Examples** N/A

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.23channel

Use this command to configure channels for the specified radio.

**channel** *channel-num*

Parameter Description	Parameter	Description
	<i>channel-num</i>	Indicates the channel ID, in the range from 1 to 14. Or frequency ID, in the range from 2412 to 2484.

**Defaults** Channel 1 is used at the 2.4 GHz band and channel 149 is used at the 5.8 GHz band.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies channel 6.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# channel 6

```

Related Commands	Command	Description
	-	-

**Platform** N/A

**Description**

## 1.24chan-width

Use this command to set the bandwidth of the specified radio.

**chan-width** { 20 | 40 | 80 | 160 }

Parameter Description	Parameter	Description
	<b>20</b>	Sets the radio width to 20 Mbps.
	<b>40</b>	Sets the radio width to 40 Mbps.
	<b>80</b>	Sets the radio width to 80 Mbps.
	<b>160</b>	Sets the radio width to 160 Mbps.

**Defaults** The default channel bandwidth of 5.8G radio is 40 Mbps.  
The default channel bandwidth of the other radio is 20 Mbps.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets the radio width of radio1 to 40 Mbps.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# chan-width 40

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.25clear dfs historical-radar-channels

Use this command to clear historical records of radar channels of APs.

**clear dfs historical-radar-channels**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command  
mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears historical records of radar channels of AP.

**Examples**

```

Hostname# clear dfs historical-radar-channels

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform  
Description** N/A

## 1.26country-code

Use this command to specify a country code. Use the **no** form of this command to remove the country code settings.

**country-code** *country-code*

**no country** *country-code*

**Parameter  
Description**

Parameter	Description
<i>country-code</i>	Indicates a country code.

**Defaults**

The country code is JP, indicating Japan.

**Command  
Mode**

Dot11radio interface configuration mode.

**Usage Guide**

Note that Channel 14 in 2.4GHz can be configured only in 802.11b mode.

The following country codes are available:

Country Code	Country
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Columbia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic

DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
EG	Germany
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong, Special Administrative Region of China
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy
JO	Jordan
JP	Japan
KP	Democratic People's Republic of Korea
KR	Korea ROC
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	North Macedonia
MO	Macao, Special Administrative Region of China
MT	Malta
MX	Mexico



MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RS	Serbia
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovak Republic
SY	Syria
SV	El Salvador
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad and Tobago
TW	Taiwan, Province of China
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

**Configuration** The following example sets the country code to JP.

**Examples** `Hostname(config)# interface dot11radio 1/0`

```
Hostname(config-if-Dot11radio 1/0)# country-code JP
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.27 coverage-area-control

Use this command to configure the transmit power of management frames. Use the **no** form of this command to restore the default transmit power.

**coverage-area-control** *power-value*

**no coverage-area-control**

**Parameter Description**

Parameter	Description
<i>power-value</i>	Indicates the transmit power for management frames, ranging from 0 to 32 dBm.

**Defaults**

The transmit power for management frames is 0, which indicates that no transmit power is configured for management frames.

**Command mode**

Dot11radio interface configuration mode.

**Usage Guide**

N/A

**Configuration Examples**

The following example sets the transmit power of management frames to 20.

```
Hostname(config)# interface dot11radio 1/0
```

```
Hostname(config-if-Dot11radio 1/0)# coverage-area-control 20
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.28dot11 wlan

Run the **dot11 wlan** command to create a WLAN. Use the **no** form of this command to delete a WLAN.

**dot11 wlan** *wlan-id*

**no dot11 wlan** *wlan-id*

### Parameter Description

Parameter	Description
<i>wlan-id</i>	Indicates a WLAN ID.

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** Up to 16 WLANs can be created.

### Configuration Examples

The following example to create a WLAN.

```

Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)#ssid test
  
```

### Related Commands

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.29ebag

Use this command to enable ebag network optimization. Use the **no** form of this command to disable ebag network optimization.

**ebag**

**no ebag**

### Parameter Description

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** This command is generally used in e-bag scenario. Use this function with caution in other scenarios.

**Configuration Examples** The following example enables ebag network optimization.

```
Hostname(config)# ebag
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.30eth-schd

Use this command to configure maximum number of Ethernet packets received at a time. Use the **no** form of this command to restore the default limit number of packets received at a time.

**eth-schd limit**

**no eth-schd**

**Parameter Description**

Parameter	Description
<i>limit</i>	Indicates the maximum number of Ethernet packets received at a time. The range is from 1 to 256.

**Defaults** The default limit value varies by AP model.

**Command mode** Global configuration mode

**Usage Guide** You can improve the network performance by raising the received Ethernet packets limit for every time, at the cost of reducing immediacy of packets of key services. With regard to applications which are multi-user concurrent and real-time sensitive, such as electronic schoolbag, requiring only ordinary networks, you are recommended to decrease the value of received Ethernet packets limit per time to 25.

**Configuration Examples** The following example sets the maximum number of the Ethernet packets received per time to 50.

```
Hostname(config)# eth-schd 50
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.31 fragment-threshold

Use this command to set a fragment threshold for a radio. Use the **no** form of this command to restore the default fragment threshold.

**fragment-threshold** *threshold-value*

**no fragment-threshold**

**Parameter Description**

Parameter	Description
<i>threshold-value</i>	Indicates the fragment threshold, ranging from 256 to 2,346 in the unit of byte.

**Defaults** The default fragment threshold is 2,346.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** The fragment threshold must be an even number.

**Configuration Examples** The following example sets the fragment threshold of radio1 to 1,538.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# fragment-threshold 1538

```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.32 fragment-burst

Use this command to enable or disable fragment bursting for a radio. Use the **no** form of this command to restore the default fragment bursting.

**fragment-burst** { **enable** | **disable** | **dynamic** }

**no fragment-burst**

**Parameter Description**

Parameter	Description
<b>enable</b>	Enables frame bursting mechanism.
<b>disable</b>	Disables frame bursting mechanism.
<b>dynamic</b>	Dynamic frame bursting mechanism.

**Defaults** Frame bursting is disabled by default.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the AP to enable frame bursting.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# fragment-burst dynamic

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.33green-field enable

Use this command to enable the green-field protection mode for the specified radio. Use the **no** form of this command to disable the green-field protection mode.

**green-field enable**

**no green-field enable**

Parameter Description	Parameter	Description
	-	-

**Defaults** By default, the green-field protection mode is disabled.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** This command is supported only for the radio on 2.4 GHz.

**Configuration** The following example enables the green-field protection mode for radio 1.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# green-field enable
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.34 interface dot11radio

Use this command to create a dot11radio sub-interface. Use the **no** form of this command to delete the dot11radio sub-interface.

```

interface dot11radio subinterface-num
no interface dot11radio subinterface-num
    
```

**Parameter Description**

Parameter	Description
<i>subinterface-num</i>	Specifies the dot11radio sub-interface number, in the range from 1 to 16.

**Defaults**

N/A

**Command mode**

Global configuration mode

**Usage Guide**

N/A

**Configuration**

The following example configures to create a dot11radio sub-interface.

**Examples**

```

Hostname(config)# interface dot11radio 1/0.1
Hostname(config-if-Dot11radio 1/0.1)#
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.35ldpc

Use this command to enable low density parity check (LDPC) coding. Use the **no** form of this command to disable LDPC coding.

**ldpc**

**no ldpc**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, LDPC coding is enabled.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables LDPC coding.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# ldpc

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.36link-check

Use this command to enable/disable link check. Use the **no** form of this command to restore the default setting.

**link-check { enable | disable }**

**no link-check { enable | disable }**

Parameter Description	Parameter	Description
	<b>enable</b>	Enables link check.
	<b>disable</b>	Disables link check.

**Defaults** Link check is disabled by default.

**Command mode** Global configuration mode



**Usage Guide** N/A

**Configuration** The following example enables link check.

**Examples** `Hostname(config)# link-check enable`

The following example disables link check.

`Hostname(config)# link-check disable`

`Hostname(config)# no link-check enable`

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.37 mcast-rate

Use this command to configure the multicast rate for WLAN. Use the no form of this command to restore the default multicast rate.

**mcast-rate** *mcast-num*

**no mcast-rate**

**Parameter Description**

Parameter	Description
<i>mcast-num</i>	Indicates WLAN multicast rate. The available rates: 1Mbps, 6Mbps, 11Mbps, 24Mbps, 54Mbps

**Defaults** The default WLAN multicast rate is 24Mbps

**Command mode** WLAN configuration mode

**Usage Guide** A multicast rate is effective only for the current AP band. If the multicast rate is not supported by the current band, the default rate is used.

**Configuration** The following example configures the multicast rate of WLAN1 to 11Mbps.

**Examples** `Hostname(config)# dot11 wlan 1`

`Hostname(dot11-wlan-config)# mcast-rate 11`

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.38mcell enable

Use this command to enable MCell.

Use the **no** form of this command to disable MCell.

**mcell enable**

**no mcell enable**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults**

This function is disabled by default.

**Command  
mode**

Dot11radio interface configuration mode.

**Usage Guide**

N/A

**Configuration**

The following example enables MCell.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# mcell enable

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.39mu-mimo enable

Use this command to enable MU-MIMO for the specified radio. Use the **no** or **default** form of this command to restore the default setting.

**mu-mimo enable**

**no mu-mimo enable**

**default mu-mimo enable**

**Parameter  
Description**

Parameter	Description
-	-

**Defaults**

MU-MIMO is enabled by default.

**Command Mode** dot11radio interface configuration mode

### Usage Guide

**Configuration** The following example disables MU-MIMO for radio 1.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# mu-mimo enable

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.40ofdma enable

Use this command to enable RF OFDMA. Use the **no** form of this command to disable OFDMA.

**ofdma enable**  
**no ofdma enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** OFDMA is enabled by default.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** Only OFDMA-supported radio can be enabled with OFDMA.

**Configuration** The following example disables OFDMA.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# no ofdma enable

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.41 peer-distance

Use this command to configure the allowable longest distance between an AP and a wireless transmission peer.

**peer-distance** *val*

Parameter Description	Parameter	Description
	<i>val</i>	Indicates the longest distance allowed by an AP, ranging from 1,000 to 24,000 m.

**Defaults** The default distance between the radio and the peer is 1,000 m.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** This configuration is not supported for all APs. This configuration needs to be performed only when the longest distance between an AP and the wireless transmission peer is greater than 1000m. The configured distance may be longer, but cannot be shorter than the actual distance.

**Configuration Examples** The following example configures the longest distance allowed by an AP to 3,000 m.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# peer-distance 3000

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.42 poe-unlimit

Use this command to forcibly release the configured PoE limit of an AP to ensure that the maximum capacity can be configured for the AP.

**poe-unlimit]**  
**no poe-unlimit**

Parameter Description	Parameter	Description
	-	-

**Defaults** The PoE is limited based on the PoE negotiation result by default.

**Command** Dot11 radio primary interface configuration mode

**Mode****Usage Guide** N/A**Configuration** The following example releases the PoE limit of Radio 1 on AP device.

```

Examples Hostname(config)# interface dot11radio 1/0
             Hostname(config-if-Dot11radio 1/0)# poe-unlimit

```

**Verification** Run the **show running-config interface dot11radio** command to display the configuration of **poe-unlimit** of a specified AP radio.**Common Errors** N/A**Platform Description** N/A

## 1.43 poe-unlimit radio-type

Use this command to forcibly release the configured PoE limit of an AP to ensure that the maximum capacity can be configured for the AP.

**poe-unlimit radio-type { 802.11a | 802.11b }**

Parameter	Parameter	Description
<b>Description</b>	<b>802.11a</b>	Indicates the 5 GHz band.
	<b>802.11b</b>	Indicates the 2.4 GHz band.

**Defaults** The PoE is limited based on the PoE negotiation result by default.**Command Mode** Global configuration mode**Usage Guide** N/A**Configuration** The following example releases the PoE limit on AP device.

```

Examples Hostname(config)# poe-unlimit radio-type 802.11a

```

**Verification** Run the **show running** command to display the configuration of **poe-unlimit** of a specified AP.**Prompts** N/A**Common Errors** N/A**Platform Description** N/A

## 1.44 poeout

Use this command to enable the PoE power supply function of an AP.

**poeout** { **enable** | **disable** | **default** }

### Parameter Description

Parameter	Description
<b>enable</b>	Enables the PoE power supply function of an AP.
<b>disable</b>	Disables the PoE power supply function of an AP.
<b>default</b>	Uses the default PoE power supply function settings of the device.

### Defaults

The default PoE power supply function settings of the device are used by default.

### Command Mode

Global configuration mode

### Default Level

N/A

### Usage Guide

This command automatically saves the configuration, without the aid of the **write** command. This command does not support the **no** and **default** forms. After **poeout default** is configured, the default PoE power supply function configuration of the device is adopted. The default settings for different APs may vary with AP models. Run the **poeout default** command to enable different APs in a group to apply respective default PoE out settings.

### Configuration Examples

The following example enables the PoE power supply function of an AP.

#### Examples

```

Hostname#config
Hostname(config)# poeout enable

```

### Verification

Run the **show poeout** command to display the configurations.

### Platform Description

Only some models of fat APs support this function.

## 1.45 power local

Use this command to configure transmit power of the specified radio.

**power local** *power-value*

### Parameter Description

Parameter	Description
<i>power-value</i>	Indicates the transmit power, ranging from 1 to 100 in the unit of %.

### Defaults

By default, the percentage of transmit power is 100%.

### Command mode

Dot11radio interface configuration mode.

### Usage Guide

N/A

**Configuration** The following example configures the transmit power to 50%.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# power local 50
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

### 1.46 quiet-mode active off coldstart

Use this command to disable the Quiet mode after the device is cold restarted.

**quiet-mode active off coldstart**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** By default, the Quiet mode is disabled.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example disables the Quiet mode after the device is cold restarted.

**Examples**

```

Hostname(config)# quiet-mode active off coldstart
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

### 1.47 quiet-mode active on coldstart

Use this command to enable the Quiet mode after the device is cold restarted.

**quiet-mode active on coldstart**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	By default, the Quiet mode is disabled.	
<b>Command mode</b>	Global configuration mode.	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example enables the Quiet mode after the device is cold restarted.	
	<code>Hostname(config)# quiet-mode active on coldstart</code>	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.48 radio-optimize

Use this command to optimize radio parameters (including the power, channel, and antenna Tx/Rx type) for a specified AP.

**radio-optimize** [{ **802.11a** | **802.11b** } { **802.11a** | **802.11b** }]

<b>Parameter Description</b>	Parameter	Description
	<b>802.11a</b>	Indicates the 5 GHz band.
	<b>802.11b</b>	Indicates the 2.4 GHz band.
<b>Defaults</b>	One-command configuration optimization is not used by default.	
<b>Command Mode</b>	Global configuration mode	
<b>Default Level</b>	14	
<b>Usage Guide</b>	When this command is configured, radio parameters are immediately modified (including the power, channel, antenna transmit/receive type) only for APs supporting one-click optimization and the command configuration is not saved (but relevant parameter modifications are saved).	



<b>Configuration</b>	The following example configures one-command configuration optimization.
<b>Examples</b>	<pre>Ruijie(config)# radio-optimize</pre> The following example changes <b>radio-type</b> via one-command configuration optimization. <pre>Ruijie(config)# radio-optimize 802.11a 802.11a</pre>
<b>Verification</b>	Run the <b>show running</b> command to display the radio parameter configuration of a specified AP (check radio parameter configuration for online APs).
<b>Prompts</b>	N/A
<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

## 1.49 radio-type

Use this command to configure the RF mode for the specified radio of the specified AP.

**radio-type {802.11a | 802.11b}**

<b>Parameter Description</b>	Parameter	Description
	<b>802.11a</b>	Indicates the 5GHz band is used.
	<b>802.11b</b>	Indicates the 2.4GHz band is used.
<b>Defaults</b>	By default, the AP device with single radio (namely, radio1) operates in 2.4 GHz, while the AP device with dual radios can operate in 2.4 GHz (radio1) and 5 GHz (radio2).	
<b>Command Mode</b>	Dot11radio interface configuration mode.	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example configures radio 1 to operates in 2.4 GHz. <pre>Hostname(config)# interface dot11radio 1/0</pre> <pre>Hostname(config-if-Dot11radio 1/0)# radio-type 802.11a</pre>	
<b>Related Commands</b>	Command	Description
	N/A	N/A
<b>Platform Description</b>	N/A	

## 1.50rate-set 11a

Use this command to configure the 802.11a rate set.

**rate-set 11a** { **mandatory** | **support** | **disable** } *speed*

Parameter Description	Parameter	Description
	<b>mandatory</b>	Indicates whether a rate is a mandatory rate.
	<b>support</b>	Indicates whether a rate is supported.
	<b>disable</b>	Indicates whether a rate is disabled.
	<i>speed</i>	Specifies a rate.

**Defaults** 6 Mbit/s, 9 Mbit/s and 12 Mbit/s are mandatory rates and all the other rates are supported rates.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 6.

```

Hostname(config)# interface dot11radio 2/0
Hostname(config-if-Dot11radio 2/0)# rate-set 11a support 6

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.51rate-set 11ac

Use this command to configure the 802.11ac rate set.

**rate-set 11ac** { **mcs-mandatory** | **mcs-support** } *index*

Parameter Description	Parameter	Description
	<b>mcs-mandatory</b>	Indicates whether a rate is a mandatory mcs rate.
	<b>mcs-support</b>	Indicates whether an mcs rate is supported.
	<i>index</i>	Specifies an mcs rate.

**Defaults** The mcs is 9 for one stream, 19 for two streams, and 29 for three streams. All mandatory mcs is 0.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 9.

```

Hostname(config)# interface dot11radio 2/0
Hostname(config-if-Dot11radio 2/0)# rate-set 11ac mcs-support 9

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.52rate-set 11ax

Use this command to configure the 802.11ax rate set.

**rate-set 11ax mcs-support** *index*

Parameter Description	Parameter	Description
	<b>mcs-support</b>	Indicates whether an mcs rate is supported.
	<i>index</i>	Specifies an mcs rate.

**Defaults** Number of supported MCS rates = (Number of radio streams x 12) – 1.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 23.

```

Hostname(config)# interface dot11radio 2/0
Hostname(config-if-Dot11radio 2/0)# rate-set 11ax mcs-support 23

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.53rate-set 11b

Use this command to configure the 802.11b rate set.

**rate-set 11b** { **mandatory** | **support** | **disable** } *speed*

Parameter Description	Parameter	Description
	<b>mandatory</b>	Indicates whether a rate is a mandatory rate.
	<b>support</b>	Indicates whether a rate is supported.
	<b>disable</b>	Indicates whether a rate is disabled.
	<i>speed</i>	Specifies a rate.

**Defaults** 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps are mandatory rates.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 5.5.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-Dot11radio 1/0)# rate-set 11b support 5

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.54rate-set 11g

Use this command to configure the 802.11g rate set.

**rate-set 11g** { **disable** | **mandatory** | **support** } *speed*

Parameter Description	Parameter	Description
	<b>mandatory</b>	Indicates whether a rate is a mandatory rate.
	<b>support</b>	Indicates whether a rate is supported.
	<b>disable</b>	Indicates whether a rate is disabled.
	<i>speed</i>	Specifies a rate.

**Defaults** 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps are mandatory rates and all the other rates are supported rates.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 5.5.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# rate-set 11g support 5
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.55rate-set 11n

Use this command to configure the 802.11n rate set.

**rate-set 11n { mcs-mandatory | mcs-support } index**

Parameter Description	Parameter	Description
	<b>mcs-mandatory</b>	
<b>mcs-support</b>		Indicates whether an mcs rate is supported.
<i>index</i>		Specifies an mcs rate.

**Defaults** The mcs is 7 for one stream, 15 for two streams, and 23 for three streams. All mandatory mcs is 0.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the rate to 7.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# rate-set 11n mcs-support 7
    
```

Related Commands	Command	Description

N/A	N/A
-----	-----

**Platform** N/A  
**Description**

## 1.56 response-rssi

Use this command to configure the minimum value of RSSI for STA access. Use the **no** form of this command to restore the default setting.

**response-rssi** *rssi-value*  
**no response-rssi**

Parameter Description	Parameter	Description
	<i>rssi-value</i>	Indicates the minimum RSSI for STA access, ranging from 0 to 100 in the unit of dBm.

**Defaults** The minimum RSSI for STA access is 0, which indicates that all STAs are allowed for access regardless of their RSSI values.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the minimum value of RSSI for STA access to 20.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# response-rssi 20
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.57rts threshold

Use this command to configure the RTS threshold of the specified radio. Use the **no** form of this command to restore the default RTS threshold.

**rts threshold** *threshold-value*  
**no rts threshold**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>threshold-value</i>	Indicates the RTS threshold, ranging from 257 to 2,347 in the unit of byte.
------------------------	---

**Defaults** The default RTS threshold is 2,347.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the RTS threshold of radio1 to 2346.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# rts threshold 2346

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.58short-gi enable chan-width

Use this command to enable the short protection interval. Use the **no** form of this command to disable the short protection interval.

**short-gi enable chan-width { 20 | 40 | 80 | 160 }**

**no short-gi enable chan-width { 20 | 40 | 80 | 160 }**

Parameter Description	Parameter	Description
	<b>20</b>	Indicates enabling/disabling the short protection interval at the channel bandwidth of 20 MHz.
<b>40</b>	Indicates enabling/disabling the short protection interval at the channel bandwidth of 40 MHz.	
<b>80</b>	Indicates enabling/disabling the short protection interval at the channel bandwidth of 80 MHz.	
<b>160</b>	Indicates enabling/disabling the short protection interval at the channel bandwidth of 160 MHz. This parameter varies with different product versions.	

**Defaults** The short protection interval is enabled at 20 MHz and 40 MHz and disabled at 80 MHz.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example enables the short protection interval at the channel bandwidth of 20 MHz.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# short-gi enable chan-width 20

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.59short-preamble

Use this command to enable the short preamble. Use the **no** form of this command to disable the short preamble.

**short-preamble**

**no short-preamble**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** The short preamble is enabled.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example disables the short preamble.

**Examples**

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# no short-preamble

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**



## 1.60 show dot11 associations

Use this command to display the session information.

**show dot11 associations** *H.H.H interface-name*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	Specifies the STA MAC address in the format of H.H.H
	<i>Interface-name</i>	Specifies a radio

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays session information of STA 0025.9c9b.aeb5.

```

Examples
Hostname# show dot11 associations 0025.9c9b.aeb5 1/0
The details of client 0cd6.bd11.7f9d.
  RSSI..... 38
  SNR..... -57
  AID..... 1
  RX Data..... 357
  RX Management..... 42
  RX Control..... 0
  RX Unicast..... 89
  RX Multicast..... 17
  RX Bytes..... 18681
  TX Data..... 9
  TX Management..... 4
  TX Unicast..... 9
  TX Multicast..... 0
  TX Bytes..... 990
  TX Probe..... 0
  TX Assoc..... 1
  TX Assoc Fail..... 0
  TX Auth..... 3
  TX Auth Fail..... 0
  TX Deauth..... 0
  TX Disassoc..... 0
  Packet Load..... 0
    
```

Related	Command	Description
---------	---------	-------------

Commands		
	N/A	N/A

**Platform** N/A  
**Description**

## 1.61 show dot11 associations all-client

Use this command to display the information of all wireless clients.

**show dot11 associations all-client**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information of all wireless clients.

```

Hostname# show dot11 associations all-client
RADIO-ID WLAN-ID ADDR          AID  CHAN  RATE_DOWN  RATE_UP
RSSI ASSOC_TIME IDLE TXSEQ  RXSEQ  ERP  STATE  CAPS  HTCAPS
VHT_MU_CAP HECAPS
1      7      00:25:9c:9b:ae:b5 1    1    52.0M      6.0M  39
0:00:18 0    7    544    0x0  0x3    ESs      SU

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.62 show dot11 channels active

Use this command to display active channels supported by a radio.

**show dot11 channel active** *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Specifies a radio in the format of radioid/0.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays active channels supported by radio1.

```

Hostname# show dot11 channel active 1/0
Channel 1 : 2412 Mhz 11ng C CU          Channel 8 : 2447 Mhz 11ng C CU
CL
Channel 2 : 2417 Mhz 11ng C CU          Channel 9 : 2452 Mhz 11ng C CU
CL
Channel 3 : 2422 Mhz 11ng C CU          Channel 10 : 2457 Mhz 11ng C CL
Channel 4 : 2427 Mhz 11ng C CU          Channel 11 : 2462 Mhz 11ng C CL
Channel 5 : 2432 Mhz 11ng C CU CL       Channel 12 : 2467 Mhz 11ng C CL
Channel 6 : 2437 Mhz 11ng C CU CL       Channel 13 : 2472 Mhz 11ng C CL
Channel 7 : 2442 Mhz 11ng C CU CL

```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.63 show dot11 channels all

Use this command to all channels supported by a radio.

**show dot11 channels all** *interface-name*

Parameter Description	Parameter	Description
	<i>interface-name</i>	Specifies a radio in the format of radioid/0.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays all channels supported by radio1.

```

Examples Hostname# show dot11 channels all 1/0
The Details of Client 0025.9c9b.aeb5:
Channel 1 : 2412 Mhz 11ng C CU          Channel 8 : 2447 Mhz 11ng C CU
CL
Channel 2 : 2417 Mhz 11ng C CU          Channel 9 : 2452 Mhz 11ng C CU
CL
Channel 3 : 2422 Mhz 11ng C CU          Channel 10 : 2457 Mhz 11ng C CL
Channel 4 : 2427 Mhz 11ng C CU          Channel 11 : 2462 Mhz 11ng C CL
Channel 5 : 2432 Mhz 11ng C CU CL       Channel 12 : 2467 Mhz 11ng C CL
Channel 6 : 2437 Mhz 11ng C CU CL       Channel 13 : 2472 Mhz 11ng C CL
Channel 7 : 2442 Mhz 11ng C CU CL
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.64show dot11 mbssid

Use this command to display the BSS list.

**show dot11 mbssid**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the BSS list.

```

Examples Hostname# show dot11 mbssid
           name: Dot11radio 1/0.1
wlan id: 1
           ssid: fat-ap
    
```

bssid: 0a0c.3067.fbbf

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.65 show dot11 radio-status

Use this command to display status and capacity of all RF ports.

**show dot11 radio-status**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays status and capacity of all RF ports.

```

Hostname#show dot11 radio-status
radio status      capability
-----
1    online      b/g/n
2    online      a/n/ac/ax
    
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.66 show dot11 rate-set

Use this command to display speed set of all RF ports.

**show dot11 rate-set**

<b>Parameter</b>	Parameter	Description

<b>Description</b>		
	N/A	N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays speed set of all RF ports.

**Examples**

```

Hostname# show dot11 rate-set
LLCB(1) RATE SET
Mandatory rate: 11M,
Support rate: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M,
Mandatory 11n MCS index:
Support 11n MCS index: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,
LLCB(2) RATE SET
Mandatory rate: 6M, 12M, 24M,
Support rate: 9M, 18M, 36M, 48M, 54M,
Mandatory 11n MCS index:
Support 11n MCS index: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15,

```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.67 show dot11 wlan

Use this command to display WLAN information and configuration.

**show dot11 wlan** *wlan-id*

<b>Parameter Description</b>	Parameter	Description
	<i>wlan-id</i>	Specifies a WLAN

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the information and configuration of WLAN 2.

```

Examples
Hostname# show dot11 wlan 2
Network Name (SSID): ssid-wlan-2
  Interface..... Dot11radio 2/0.2
  Vlan (group) id..... 0
  MAC Address..... 0e14.5876.675b
  Beacon Period..... 100
  RTS Threshold..... 2347
  Fragment Threshold..... 2346
  Radio Mode..... 11ac_vht20_5g
  Channel..... 5825(165)
  Noise Floor..... -107 dBm
  Channel width..... 20Mhz
  Current Tx Power Level..... 100%
  Mcast rate ..... 24
  Current CCA ..... 28

Tx/Rx Chain:
  Antenna Gain..... 3
  Tx Chain Mask..... 0x3
  Num of Antenna Tx..... 2
  Rx Chain Mask..... 0x3
  Num of Antenna Rx..... 2

Power Save:
  DTIM Period..... 1
  DTIM Count..... 0
  Stations In Power Save..... 0
  Stations Total..... 0

11n Aggregation:
  A-mpdu Status..... Enable

Tx Retries:
  Tx short   retries..... 7
  Tx long   retries..... 4

Total Stations:
  Total..... 0
  Non-ERP..... 0
  Non-HT..... 0
  HT20..... 0
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.68show dot11 wireless

Use this command to display the information and configuration of a radio.

**show dot11 wireless** *interface-num*

Parameter Description	Parameter	Description
	<i>interface-num</i>	Specifies a radio in the format of radioid/0.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the information and configuration of radio 1.

```

Hostname# show dot11 wireless 1/0
Network Name (SSID): NULL
  Interface..... Dot11radio 1/0
  Vlan (group) id..... 0
  MAC Address..... 000c.3067.fbbf
  Beacon Period..... 100
  RTS Threshold..... 2347
  Fragment Threshold..... 2346
  Radio Mode..... 11ng_ht20
  Channel..... 2412(1)
  Noise Floor..... -103 dBm
  Channel width..... 20Mhz
  Current Tx Power Level..... 100%
  Current CCA ..... 28
Tx/Rx Chain:
  Antenna Gain..... 3
  Tx Chain Mask..... 0x3
  Num of Antenna Tx..... 2
  Rx Chain Mask..... 0x3
  Num of Antenna Rx..... 2
Power Save:
  DTIM Period..... 1
  DTIM Count..... 0
  Stations In Power Save..... 0
    
```



```

Stations Total..... 0
11n Aggregation:
  A-mpdu Status..... Enable
Tx Retries:
  Tx short   retries..... 7
  Tx long    retries..... 4
Total Stations:
  Total..... 0
  Non-ERP..... 0
  Non-HT..... 0
  HT20..... 0
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.69 show ebag

Use this command to display Ebag information and configuration.

**show ebag**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults**

N/A

**Command mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration Examples**

The following example displays Ebag information and configuration.

```

Hostname# show ebag
auto ebag status: disable
    
```

**Related Commands**

Command	Description
N/A	N/A

**Platform**

N/A

## Description

## 1.70 slottime

Use this command to enable the short slot time. Use the **no** form of this command to disable the short slot time.

**slottime** { **long** | **short** }

## Parameter Description

Parameter	Description
<b>long</b>	Indicates the long time slot.
<b>short</b>	Indicates the short time slot .

**Defaults** By default, short slot time is enabled.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables short slot time.

```

Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# slottime long

```

## Related Commands

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.71 ssid

Use the **ssid** command to configure the SSID of a specified WLAN.

Use the **no** form of this command to restore the default setting.

**ssid** *ssid-string*

**no ssid** *ssid-string*

## Parameter Description

Parameter	Description
<i>ssid-string</i>	Specifies an SSID string containing up to 32 characters.

**Defaults** N/A

**Command Mode** WLAN configuration mode

**Usage Guide** N/A

**Configuration Example** The following example to create a WLAN.

```
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# ssid test
```

**Platform Description** N/A

## 1.72 sta-idle-timeout

Use this command to configure the STA idle time. Use the **no** form of this command to restore the default setting.

**sta-idle-timeout** *seconds*  
**no sta-idle-timeout**

Parameter Description	Parameter	Description
	<i>seconds</i>	Indicates the STA idle time, ranging from 60 to 86,400 seconds.

**Defaults** The default is 300 seconds.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** If no information is received from an STA within the setting time, the wireless user will be regarded to have left the WLAN, and will be deleted from the network.

**Configuration Examples** The following example configure STA idle time to 600 seconds.

```
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# sta-idle-timeout 600
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.73 sta-limit

Use this command to configure the maximum number of STAs in a WLAN.

Use the **no** form of this command to restore the default setting.

**sta-limit** *num*

**no sta-limit** *num*

**Parameter  
Description**

Parameter	Description
<i>num</i>	Indicates the maximum number of STAs that can access a WLAN.

**Defaults**

The default value and range vary with different product versions..

**Command**

WLAN configuration mode

**mode**

Dot11radio interface configuration mode

Global configuration mode

**Usage Guide**

This command is used to configure the maximum number of STAs in a WLAN.

**Configuration**

The following example configures the maximum number of STAs to 20.

**Examples**

```

Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# sta-limit 20

```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.74 stbc

Use this command to enable space-time block code (STBC). Use the **no** form of this command to disable STBC.

**stbc**

**no stbc**

**Parameter  
Description**

Parameter	Description
N/A	N/A

**Defaults** By default, STBC is enabled.

**Command mode** Dot11radio interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables STBC.

```
Hostname(config)# interface dot11radio 1/0
Ruijie (config-if-Dot11radio 1/0)# stbc
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.75 txbf enable

Use this command to enable beamforming. Use the **no** form of this command to disable beamforming.

**txbf enable**

**no txbf enable**

**Parameter Description**

Parameter	Description
<b>no</b>	Disables beamforming.

**Defaults** Beamforming is enabled by default.

**Command mode** Dot11radio interface configuration mode

**Usage Guide** After TxBF beamforming is enabled, the transmit end adjusts the WLAN signal emitting mode according to the evaluated channel status of the received end, aims at the antenna, and make the signal reach the receive end with the highest strength, thereby improving transmission rate and throughput of WLAN links.

**Configuration Examples** The following example enables beamforming.

```
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# txbf enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.76 wlan-id

Use this command to configure the WPS quick access. Use the **no** form of this command to restore the default setting.

**wlan-id** *wlan-id*  
**no wlan-id**

Parameter Description	Parameter	Description
	<i>wlan-id</i>	

**Defaults** N/A

**Command mode** Dot11radio sub-interface configuration mode

**Usage Guide** N/A

**Configuration** The following example configures the WLAN ID that is mapped to a dot11radio interface.

**Examples**

```

Hostname(config)#interface Dot11radio 1/0.1
Hostname(config-subif-Dot11radio 1/0.1)#wlan-id 1

```

Related Commands	Command	Description
	<b>dot11 wlan</b>	
<b>interface dot11radio</b>		Create or delete the dot11 radio sub-interface
<b>encapsulation dot1Q</b>		Configure the VLAN attributes of the specified dot11 radio sub-interface

<b>Platform</b>	N/A
<b>Description</b>	

## 1.77 quiet-mode session

Use this command to configure LED quiet mode.

Use the **no** form of this command to restore the default setting.

**quiet-mode session** *session-num*

**no quiet-mode session** *session-num*

Parameter Description	Parameter	Description
	<i>session-num</i>	Session ID.

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to turn off all LEDs on the AP.

**Configuration** The following example configures LED quiet mode from 23:00 that night to 7:00 next day.

**Examples**

```

Hostname(config)#schedule session 1
Hostname(config)#schedule session 1 time-range 1 period Mon time
23:00 to 7:00
Ruijie(config)#quiet-mode session 1

```

The following example disables LED quiet mode.

```

Hostname(config)#no quiet-mode session 1

```

**Platform Description** N/A



# 1 STA Management Commands

## 1.1 ap

Use this command to configure the AP information in the association control zone. Use the **no** form of this command to delete the specified AP from the association control zone.

**ap** *ap-name*

**no ap** [ *ap-name* ]

Parameter Description	Parameter	Description
	<i>ap-name</i>	AP name. The name length range is from 1 to 64.

**Defaults** No AP information in the association control zone is configured by default.

**Command mode** Association control zone configuration mode

**Usage Guide** If the AP works in the fat or MACC mode, configure *ap-name* as the hostname of the AP.

**Configuration Examples** The following example configures a set of AP information with MAC address of 00d0.f800.1001 for an association control zone named "Class(1)Grade1".

```

Hostname(config)#control-zone Class(1)Grade1
Hostname(config-cznoe)# ap 00d0.f800.1001

```

Related Commands	Command	Description
	<b>show control-zone</b>	Displays the association control zone.

**Platform Description** N/A

## 1.2 assoc-control

Use this command to enable the association control function. Use **no** form of this command to restore the default setting.

**assoc-control**

**no assoc-control**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

**Defaults** This function is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** When the association control function is disabled, the association control related commands can still be configured with the ineffective association control function.

**Configuration Examples** The following example enables the association control function.

```
Hostname(config)# assoc-control
```

The following example disables the association control function.

```
Hostname(config)# no assoc-control
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.3 control-zone

Use this command to create an association control zone and enter association control zone configuration mode. Use the **no** form of this command to restore the default setting.

**control-zone** *czone-name*

**no control-zone** [ *czone-name* ]

**Parameter Description**

Parameter	Description
<i>czone-name</i>	Association control zone name. The name length range is 1 to 64.

**Defaults** No association control zone is configured by default.

**Command mode** Global configuration mode

**Usage Guide** Only one association control zone is allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

**Configuration Examples** The following example configures an association control zone named "Class (1) Grade1".

```
Hostname(config)# control-zone Class(1)Grade1
Hostname(config-czone)#
```

The following example deletes an association control zone named “Class(1)Grade1”.

```

Hostname(config)# no control-zone Class(1)Grade1
The operation will clear the control zone configuration, which may cause
corresponding STAs offline. Continue? [no] y
Hostname(config)#
    
```

<b>Related Commands</b>	Command	Description
	<b>show control-zone summary</b>	Displays the summary of association control zones.

**Platform** FAT AP  
**Description**

### 1.4 hide-ssid sta-reach-limit

Use this command to hide the SSID when the number of STAs associated with the AP reaches the limit. Use the **no** form of this command to restore the default setting.

```

hide-ssid sta-reach-limit
no hide-ssid sta-reach-limit [ radio { 2.4g | 5g } ]
    
```

<b>Parameter Description</b>	Parameter	Description
	<b>radio</b>	Enables this function on the specified radio. If no radio is specified, it is enabled on both radio.
	<b>2.4g</b>	Enables this function on 2.4G radio.
	<b>5g</b>	Enables this function on 5G radio.

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After the intelligent SSID function is enabled and the numbers of STAs on all APs in an area reach the upper limit, new STAs cannot detect the SSID in this area.

**Configuration Examples** The following example hides the SSID for 5G radio when the number of STAs associated with the AP reaches the limit.

```

Hostname(config)# hide-ssid sta-reach-limit
    
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.5 inter-radio-balance num-balance dual-band

Use this command to configure the enabling threshold and balancing threshold for STA balancing between the different radios (2.4G and 5.0G) of AP devices. Use the **no** form of this command to restore the default settings.

**inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*

**no inter-radio-balance num-balance dual-band**

**Parameter Description**

Parameter	Description
<i>en-num</i>	The enabling threshold value. Load balancing is enabled only when the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 100.
<i>thrs-num</i>	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio and lowest load radio. The range is from 1 to 100.

**Defaults** By default, the enabling threshold is 20 and the balancing threshold is 8.

**Command mode** Global configuration mode

**Usage Guide** When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs will be balanced to radio of lower load. This configuration takes effect only when the radio of lowest load is on the different radio to be associated. The **inter-radio-balance num-balance same-band** takes effect If the two radios are on the same radio.

**Configuration Examples** The following example configures the enabling threshold and balancing threshold to 10 and 10 respectively for the different radios.

```
Hostname(config)# inter-radio-balance num-balance dual-band enable-load 10 threshold 10
```

The following example restores the default load balancing settings for different radios.

```
Hostname(config)# no inter-radio-balance num-balance dual-band
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.6 inter-radio-balance num-balance enable

Use this command to enable load balancing for the number of STAs between different radios (2.4G and 5.0G) on the AP device.

Use the **no** form of this command to disable load balancing between radios on the AP device.

**inter-radio-balance num-balance enable**

**no inter-radio-balance num-balance enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** By default, load balancing between radios is disabled.

**Command mode** Global configuration mode

### Usage Guide

**Configuration** The following example disables load balancing for the number of STAs between radios.

**Examples**

```
Hostname(config)# no inter-radio-balance num-balance enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.7 inter-radio-balance num-balance same-band

Use this command to configure the enabling threshold and balancing threshold for STA balancing between the same radios (both 2.4G or 5.0G) of AP devices.

Use the **no** form of this command to restore the default settings.

**inter-radio-balance num-balance same-band enable-load *en-num* threshold *thrs-num***

**no inter-radio-balance num-balance same-band**

Parameter Description	Parameter	Description
	<i>en-num</i>	The enabling threshold value. Load balancing is enabled only when the number of STAs associated with the radio exceeds the threshold. The range is from 1 to 100.
	<i>thrs-num</i>	The balancing threshold value. The STA will be disassociated with the radio when the STA number difference between the associated radio

	and lowest load radio. The range is from 1 to 100.
--	--

**Defaults** By default, the enabling threshold is 20 and the balancing threshold is 6.

**Command mode** Global configuration mode

**Usage Guide** When the load balancing between radios is enabled, if the number of STAs associated with the radio exceeds the enabling threshold and the STA number difference between the associated radio and lowest load radio exceeds the balancing threshold, the STA will be disassociated with the radio and the STAs will be balanced to the radio of lower load. This configuration takes effect only when the radio of lowest load is on the different the radio to be associated. The **inter-radio-balance num-balance dual-band** takes effect If the two radios are on the different radio.

**Configuration Examples** The following example configures the enabling threshold and balancing threshold to 3 and 3 respectively for the same radios on AP.

```
Hostname(config)# inter-radio-balance num-balance same-band enable-load 3
threshold 3
```

The following example restores the default load balancing settings for the same radios.

```
Hostname(config)# no inter-radio-balance num-balance same-band
```

**Platform Description**

## 1.8 inter-radio-balance radio weight

Use this command to configure the weight for load balancing among radio.

Use the **no** form of this command to restore the default setting.

**inter-radio-balance radio** *radio-id* **weight** *weight-num*

**no inter-radio-balance radio** *radio-id* **weight**

Parameter Description	Parameter	Description
	<i>radio-id</i>	Specifies a radio.
	<i>weight-num</i>	Configures the weight, in the range from 1 to 100.

**Defaults** The default weight is 100, that is, radio 1: radio 2=100:100 (1:1).

**Command mode** Global configuration mode

**Usage Guide** If you want to configure radio 1: radio 2= 50:100 (1:2). please set the weight of radio 1 to 50,

**Configuration** The following example sets the weight of radio 1 to 50, that is, radio 1: radio 2=50:100 (1:2).

**Examples** `Hostname(config)# inter-radio-balance radio 1 weight 50`

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.9 package

Use this command to create a terminal package and enter terminal package configuration mode. Use the **no** form of this command to restore the default setting.

**package** *pkg-name*

**no package** [ *pkg-name* ]

**Parameter  
Description**

Parameter	Description
<i>pkg-name</i>	Terminal package name. The name length range is from 1 to 32.

**Defaults** No terminal packets are configured by default.

**Command  
mode** Global configuration mode

**Usage Guide** Only 50 terminal packages are allowed to be configured on a fat AP. The system will prompt an error message if the upper limit is exceeded.

**Configuration** The following example configures a terminal package named "Cart1".

**Examples** `Hostname(config)#package Cart1`  
`Hostname(config-package)#`

The following example configures the package named "Cart1".

```
Hostname(config)# no package Cart1
The operation will clear package(s) configuration, which may cause
corresponding STAs offline. Continue? [no] y
Hostname(config)#
```

**Related  
Commands**

Command	Description
<b>show package</b>	Displays the terminal package configuration.

**Platform** FAT AP  
**Description**

## 1.10 primary-sta

Use this command to configure a primary STA in a terminal package. Use the **no** form of this command to remove the configuration.

**primary-sta** *mac-address*

**no primary-sta**

Parameter Description	Parameter	Description
	<i>mac-address</i>	The MAC address of the primary STA, in the format of H.H.H.

**Defaults** N/A

**Command mode** Package configuration mode

**Usage Guide** A terminal package can be configured up to one primary STA. Therefore the newly configured primary STA will cover the one which has been configured in a terminal packet.

**Configuration Examples** The following example configures a primary STA with MAC address of 00d0.f800.0001 for the terminal package "Cart1".

```

Hostname(config)# package Cart1
Hostname(config-package)#primary-sta 00d0.f800.0001

```

Related Commands	Command	Description
	<b>show package</b>	Displays the terminal package configuration.

**Platform** FAT AP

**Description**

## 1.11 secondary-sta

Use this command to configure secondary STAs in a terminal package. Use the **no** form of this command to remove the configuration.

**secondary-sta** *mac-address*

**no secondary-sta** [*mac-address*]

Parameter Description	Parameter	Description
	<i>mac-address</i>	The MAC address of the secondary STA, in the format of H.H.H.

**Defaults** N/A

**Command** Package configuration mode



**mode**

**Usage Guide** Up to 100 secondary STAs can be configured in one terminal package. The system will prompt the error message in the following conditions if you use this command to configure the secondary STA:  
 The secondary STA configured has existed in the terminal package.  
 The number of STAs in a terminal package exceeds 100.

**Configuration Examples** The following example configures a secondary STA with MAC address of 00d0.f800.0002 for the package "Cart 1".

```

Hostname (config) #package Cart1
Hostname (config-package) #secondary-sta 00d0.f800.0002
    
```

Related Commands	Command	Description
		<b>show package</b>

**Platform** FAT AP  
**Description**

## 1.12 show assoc-control

Use this command to display the state of the association control.  
**show assoc-control**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the state of the association control.

```

Hostname# show assoc-control
Association control is enabled.
    
```

Related Commands	Command	Description
		N/A

**Platform** FAT AP

**Description****1.13 show control-zone**

Use this command to display the association control-zone configuration.

**show control-zone** [ **summary** | *czone-name* ]

Parameter Description	Parameter	Description
	<b>summary</b>	Displays summary information.
	<i>czone-name</i>	The name of the association control-zone to be displayed. The name length range is from 1 to 64.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use the **show control-zone summary** command to display the configured association control zone. Use the **show control-zone** or the **show control-zone czone-name** command to display not only the association control zone information but also the AP information in the control zone.

**Configuration Examples** The following example displays all association control zones.

```

Hostname# show control-zone summary
control zone num : 1
Classroom1

```

The following example displays the detailed configuration information of all the association control zones.

```

Hostname(config)# show control-zone
control zone num : 1
Control zone    AP
-----
Classroom1     AP850-IV2                5869.6c1a.ce12

```

The following example displays the detailed configuration information of all association control zone.

```

Hostname# show control-zone
No control zone configuration.

```

The following example displays the detailed configuration information of the association control zone named "Class1Grade1".

```

Hostname(config)# show control-zone Classroom1
control zone num : 1
Control zone    AP
-----
Classroom1     AP850-IV2                5869.6c1a.ce12

```

Related Commands	Command	Description
	<b>control-zone</b>	Configures an association control zone and enter association control zone configuration mode.
	<b>ap</b>	Configures AP information in the association control zone.

**Platform** FAT AP  
**Description**

### 1.14 show package

Use this command to display the terminal package configuration.

**show package** [ *pkg-name* ]

Parameter Description	Parameter	Description
	<i>pkg-name</i>	The name of the terminal package to be displayed. The name length range is from 1 to 32.

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration of all terminal packages.

```

Hostname# show package
total package num: 2
===== Cart1 =====
Primary STA: 00d0.f800.0001
Secondary STA num : 2
00d0.f800.0003
00d0.f800.0002
===== pkg =====
Primary STA: none
Secondary STA num : 0
    
```

Related Commands	Command	Description
	<b>package</b>	Enters terminal package configuration mode
	<b>primary-sta</b>	Configures a primary STA.

<b>secondary-sta</b>	Configures a secondary STA.
----------------------	-----------------------------

**Platform** FAT AP

**Description**

## 1.15 sta-behaviour dhcp-proxy delay

Use this command to configure DHCP proxy delay time. Use the **no** form of this command to restore the default setting.

**sta-behaviour dhcp-proxy delay** *time*

**no sta-behaviour dhcp-proxy delay**

Parameter Description	Parameter	Description
	<i>time</i>	Configures DHCP proxy delay time in seconds. The range is from 1 to 60.

**Defaults** N/A

**Command mode** AC configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures DHCP proxy delay time to one second.

**Examples**

```
Hostname(config)# sta-behaviour dhcp-proxy delay 1
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.16 sta-behaviour dhcp-proxy enable

Use this command to enable DHCP proxy. Use the **no** form of this command to disable DHCP proxy.

**sta-behaviour dhcp-proxy enable**

**no sta-behaviour dhcp-proxy enable**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

N/A	N/A
-----	-----

**Defaults** DHCP proxy is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables DHCP proxy.

**Examples**

```
Hostname(config)# sta-behaviour dhcp-proxy enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.17 sta-behaviour ip-check delay

Use this command to configure IP check delay time. Use the **no** form of this command to restore the default settings.

**sta-behaviour ip-check delay** *time*

**no sta-behaviour ip-check delay**

Parameter Description	Parameter	Description
	<i>time</i>	

**Defaults** The default IP check delay time is 30 seconds.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example configures IP check delay time to 20 seconds.

**Examples**

```
Hostname(config)# sta-behaviour ip-check delay 20
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.18 sta-behaviour ip-check enable

Use this command to enable IP check. Use the **no** form of this command to disable IP check.

**sta-behaviour ip-check enable**

**no sta-behaviour ip-check enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** IP check is enabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables IP check.

**Examples**

```
Hostname(config)# sta-behaviour ip-check enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.19 sta-behaviour ip-check sulk

Use this command to configure IP check silence time. Use the **no** form of this command to restore the default settings.

**sta-behaviour ip-check sulk *time***

**no sta-behaviour ip-check sulk**

Parameter Description	Parameter	Description
	<i>time</i>	Configures the IP check silence time in seconds. The range is from 0 to 86400. The STA forced offline during last IP check will not be checked again during this period.

**Defaults** The default IP check silence time is 600 seconds.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example configures IP check silence time to 100 seconds.

**Examples**

```
Hostname(config)# sta-behaviour ip-check sulk 100
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.20 sta-idle-timeout

Use this command to configure aging time for a wireless user in a specified AP or AP group. Use the **no** form of this command to restore the default setting.

**sta-idle-timeout** *timer-num*

**no sta-idle-timeout**

Parameter	Description
<b>Description</b> <i>timer-num</i>	Indicates that you set the aging time, in the range from 60 to 86400 in the unit of seconds.

**Defaults** The default is 300 seconds.

**Command  
Mode** Dot11radio interface configuration mode

**Usage Guide** If no information is received from a wireless user within the setting time, the wireless user will be regarded to have left the WLAN, and will be deleted from the network by the system.

The following example enters the configuration mode of AP0001 to configure its client timeout timer to 600 seconds.

**Configuration  
Examples**

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# int dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# sta-idle-timeout 60
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.21 sta-limit

Use this command to configure the maximum number of wireless users that can be connected.

**sta-limit** *client-num*

Use the **no** form of this command to restore the default setting.

**no sta-limit** *client-num*

Parameter	Parameter	Description
Description	<i>client-num</i>	Indicates the maximum number of wireless users that can be connected.

### Defaults

The default for the online APs is determined by the AP model.

In the WLAN configuration mode, the default is no limit.

### Command Mode

Global configuration mode

WLAN configuration mode

Dot11radio interface configuration mode

### Usage Guide

This command is used to configure how many clients the device can serve at most. This value should not exceed the maximum STA number supported by an AP. The maximum number of wireless users that can be supported varies with AP products.

### Configuration Examples

The following example configures an AP to provide service for 100 clients at most.

```
Hostname(config)# sta-limit 100
```

### Related Commands

Command	Description
N/A	N/A

### Platform Description

N/A





# RF Management Commands

---

1. Band Selection Commands
2. HE Radio Selection Commands
3. RF Scheduling Commands
4. Wireless Location Commands

# 1 Band Selection Commands

## 1.1 band-select acceptable-rssi

Use this command to configure an acceptable STA RSSI lower limit. Use the **no** form of this command to restore the default setting.

**band-select acceptable-rssi** *value*

**no band-select acceptable-rssi**

Parameter Description	Parameter	Description
	<i>value</i>	Indicates acceptable STA RSSI lower limits, in the range from -100 to -50 in the unit of dBm.

**Defaults** The default is -80 dBm.

**Command Mode** Global configuration mode

**Usage Guide** This lower limit value is used to differentiate associable STAs from non-associable STAs. If the RSSI value is greater than this value, such STAs are associable and their information will be paid attention to. If the RSSI value is less than this value, the information of such STAs will be ignored. It is not recommended that users modify the default value.

**Configuration** The following example sets the acceptable STA RSSI low limit to -70dBm.

**Examples**

```
Hostname(config)# band-select acceptable-rssi -70
```

**Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.

Run the **show running-config** command to check whether the Band Select function is enabled.

Related Commands	Command	Description
	<b>show band-select configuration</b>	Displays the Band Select configuration.

**Platform Description** N/A

## 1.2 band-select access-denial

Use this command to set the access-denial count. Use the **no** form of this command to restore the

default setting.

**band-select access-denial** *value*


**no band-select access-denial**

Parameter Description	Parameter	Description
	<i>value</i>	Sets the access-denial count, in the range from 0 to 10.

**Defaults** The default is 2.

**Command Mode** Global configuration mode

**Usage Guide** The value **n** indicates that the AP does not respond until it receives **n** consecutive link authentication requests from the dual-band STA on 2.4-GHz band.

 This parameter can increase the navigation rate for high frequency spectrum, but it may cause difficulty in access to some dual-band STAs.

**Configuration Examples** The following example sets the access-denial count to 4.

```
Hostname(config)# band-select access-denial 4
```

**Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.

Run the **show running-config** command to check whether the Band Select function is enabled.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.3 band-select age-out

Use this command to configure the aging cycle of STA information. Use the **no** form of this command to restore the default setting.

**band-select age-out** { **dual-band** *value* | **suppression** *value* }

**no band-select age-out** { **dual-band** | **suppression** }


Parameter Description	Parameter	Description
	<b>dual-band</b> <i>value</i>	The aging cycle of dual-band STA information, in the range from 20 to 120 in the unit of seconds.

<b>suppression</b> <i>value</i>	The aging cycle of suppressed STA information, in the range from 10 to 60 in the unit of seconds.
---------------------------------	---

**Defaults** The default aging cycle of dual-band STA information is 60 seconds.  
 The default aging cycle of suppressed STA information is 20 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The AP is less sensitive to the STA band switching as the life cycle of the dual-band STA information increases. If the wireless users' network cards often switch between 2.4-GHz and 5-GHz bands, a smaller value can be configured; otherwise, a bigger value can be configured.

 It is recommended to configure the aging cycle of dual-band STA information as two or three times as that of the suppressed STAs.

**Configuration Examples** The following example sets the aging cycle of dual-band STA information to 120 seconds.

```
Hostname(config)# band-select age-out dual-band 120
```

The following example sets the aging cycle of suppressed STA information to 60 seconds.

```
Hostname(config)# band-select age-out suppression 60
```

**Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.  
 Run the **show running-config** command to check whether the Band Select function is enabled.

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.4 band-select enable

Use this command to enable the spectrum navigation. Use the **no** form of this command to restore the default setting.

**band-select enable**  
**no band-select enable**

Parameter Description	Parameter	Description
	N/A	N/A


**Defaults** This function is disabled by default.

**Command** WLAN configuration mode  
**Mode**

**Usage Guide** Enabling the spectrum navigation requires that:

1. WLAN is mapped to a dual-band AP.
2. WLAN is mapped to two radios of the dual-band AP.

If the scenario cannot meet the above requirements, it is recommended not to enable the spectrum navigation.

 If the WLAN with the spectrum navigation enabled is mapped to a single-band 2.4GHz AP, the dual-band STA within AP signal coverage cannot navigate to the 5GHz band.

**Configuration** The following example enables the spectrum navigation for WLAN 1.

**Examples**

```

Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# band-select enable

The following example disables the spectrum navigation for WLAN1.
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# no band-select enable
    
```

**Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.  
 Run the **show running-config** command to check whether the Band Select function is enabled.

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.5 band-select probe-count


Use this command to configure the probe count of the suppressed STAs. Use the **no** form of this command to restore the default setting.

**band-select probe-count** *value*  
**no band-select probe-count**

**Parameter Description**

Parameter	Description
<i>value</i>	Indicates the probe-count of the suppressed STAs, in the range is from 1 to 10.

- Defaults** The default is 2.
- Command Mode** Global configuration mode
- Usage Guide** This item indicates the extent of suppression to a suppressed STA: The value **n** indicates that the AP respond once after a STA transmits **n** probe requests.

 If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value.

**Configuration Examples** The following example sets the probe count of the suppressed STAs to 1.

```
Hostname(config)# band-select probe-count 1
```

- Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.
- Run the **show running-config** command to check whether the Band Select function is enabled.

**Related Commands**

Command	Description
<b>show band-select configuration</b>	Displays the Band Select configuration.

- Platform** N/A
- Description**

## 1.6 band-select scan-cycle

Use this command to configure the aging scanning cycle of STA information. Use the **no** form of this command to restore the default setting.

**band-select scan-cycle** *period*

**no band-select scan-cycle**


**Parameter Description**

Parameter	Description
<i>period</i>	Indicates the aging scanning cycle, in the range from 1 to 1000 in the unit of milliseconds.

**Defaults** The default is 200 milliseconds.

**Command Mode** Global configuration mode

**Usage Guide** A bigger aging scanning cycle value degrades the Band Select performance, but it can save the system resources.

 If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, this parameter should be set to a smaller value.

**Configuration** The following example sets the aging scanning cycle to 1 millisecond.

**Examples** `Hostname(config)# band-select scan-cycle 1`

**Verification** Run the **show band-select configuration** command to display parameters of the Band Select function.  
Run the **show running-config** command to check whether the Band Select function is enabled.

Related Commands	Command	Description
	<b>show band-select configuration</b>	Displays the Band Select configuration.

**Platform** N/A  
**Description**

## 1.7 show band-select configuration

Use this command to display the Band Select configuration.  
**show band-select configuration**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to show all configurations of the Band Select function.

**Configuration** The following example displays the Band Select configuration.

**Examples**

```

Hostname# show band-select configuration
Band Select Configuration
  Access denial..... 2
  Probe Cycle Count..... 2
  Scan Cycle Period Threshold (milliseconds)..... 40
  Age Out Suppression (seconds)..... 20
  Age Out Dual Band (seconds)..... 60
  Acceptable Client RSSI (dBm)..... -80
    
```

```
Band Select He-radio Configuration
  He-radio Access denial..... 3
  He-radio Probe Count..... 2
```

Field	Description
Acceptable Client RSSI (dBm)	Minimum RSSI for the Band Select Function
Access denial	Rejecting Count for a Dual-Band STA's 2.4 GHz Access Requests
Age Out Dual Band (seconds)	Aging Time of dual-band STA Information
Age Out Suppression (seconds)	Aging Time of inhibition STA Information
Probe Cycle Count	Probe Count of an Inhibition STA
Scan Cycle Period Threshold (milliseconds)	Scanning Cycle Threshold of an STA
He-radio Access denial	Number of Times That HE Radio Selection Rejects an STA
He-radio Probe Count	Number of Times That the HE Radio Selection Function Suppresses an STA

**Related Commands**

Command	Description
<b>show band-select statistics</b>	Displays the Band Select statistics.

**Platform** N/A  
**Description**

### 1.8 show band-select statistics

Use this command to display the Band Select statistics.

**show band-select statistics**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the Band Select statistics.

**Configuration** The following example displays the Band Select statistics.

**Examples**

```
Hostname# show band-select statistics
Band Select Statistics
```



```

Number of dual band client..... 39
Number of dual band client added..... 31669
Number of dual band client expired..... 31630
Number of suppressed client..... 7
Number of suppressed client added..... 48496
Number of suppressed client expired..... 48489

Band Hsta Select Statistics
Number of hsta probe supress..... 0
Number of nhsta probe supress..... 0
Number of hsta probe supress expired..... 0
Number of nhsta probe supress expired..... 0
Number of hsta access supress..... 0
Number of nhsta access supress..... 0
Number of hsta access supress expired..... 0
Number of nhsta access supress expired..... 0
    
```

**Related  
Commands**

Command	Description
<b>show band-select configuration</b>	Displays the Band Select configuration.

**Platform  
Description**

N/A

# 1 HE Radio Selection Commands

## 1.1 band-optimize he-radio enable

Use this command to enable the high-efficiency (HE) radio selection function and configure the HE radio selection mode (auto mode or fixed mode).

Use the **no** form of this command to disable the HE radio selection function.

Use the **default** form of this command to restore the default setting (disabled).

**band-optimize he-radio enable [ auto | fixed ]**

**no band-optimize he-radio enable**

**default band-optimize he-radio enable**

Parameter Description	Parameter	Description
	<b>auto</b>	Automatically adjusts the selection policy based on the load usage of a radio.
	<b>fixed</b>	Forcibly navigate HIGH-STAs to HE radios when the HE radio selection function is enabled, which is not changed due to RF environment differences.

**Defaults** The HE radio selection function is disabled by default.

**Command Mode** Fat AP: Global configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration Examples** The following example enables the HE radio selection function for AP "wlan-ap-001".

```
Hostname(config)# band-optimize he-radio enable auto
```

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform Description** This command is supported on fat APs.

## 1.2 band-optimize he-radio mode

Use this command to configure the type of STAs that access HE radios.

Use the **no** form of this command to enable HE radio selection to lead 802.11ax STAs to HE radios only.

Use the **default** form of this command to restore the default setting.

**band-optimize he-radio mode { 11axonly | 11ac\_11ax }**

**no band-optimize he-radio mode**

**default band-optimize he-radio mode**

Parameter Description	Parameter	Description
	<b>11axonly</b>	Leads only 802.11ax STAs to HE radios.
	<b>11ac_11ax</b>	Leads only 802.11ac and 802.11ax STAs to HE radios.

**Defaults** The default mode is **11axonly**.

**Command Mode** Fat AP: Global configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration Examples** The following example enables HE radio selection to lead 802.11ax STAs to HE radios only.

```
Hostname(config)# band-optimize he-radio mode 11axonly
```

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform Description** This command is supported on fat APs.

## 1.3 band-select he-radio access-denial

Use this command to configure the number of times that a non-HE radio rejects access requests from a HIGH-STA.

Use the **no** form of this command to restore the default setting.

**band-select he-radio access-denial access-denial-time**

[ **no** | **default** ] **band-optimize he-radio access-denial**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>access-denial-time</i></td> <td>Number of times that a non-HE radio rejects access requests from a HIGH-STA, ranging from 0 to 10.</td> </tr> </tbody> </table>	Parameter	Description	<i>access-denial-time</i>	Number of times that a non-HE radio rejects access requests from a HIGH-STA, ranging from 0 to 10.
Parameter	Description				
<i>access-denial-time</i>	Number of times that a non-HE radio rejects access requests from a HIGH-STA, ranging from 0 to 10.				
<b>Defaults</b>	2				
<b>Command Mode</b>	Global configuration mode				
<b>Default Level</b>	15				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	<p>The following example sets the number of times that a non-HE radio rejects access requests from a HIGH-STA to 4.</p> <pre>Hostname(config)# band-select he-radio access-denial 4</pre>				
<b>Verification</b>	N/A				
<b>Prompts</b>	N/A				
<b>Common Errors</b>	N/A				
<b>Platform Description</b>	This command is supported on fat APs.				

## 1.4 band-select he-radio probe-count

Use this command to configure the number of times that a non-HE radio rejects probe requests from a HIGH-STA.

Use the **no** form of this command to restore the default setting.

**band-select he-radio probe-count** *probe-count*

[ **no** | **default** ] **band-optimize he-radio probe-count**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>probe-count</i></td> <td>Number of times that a non-HE radio rejects probe requests from a HIGH-STA, ranging from 0 to 10.</td> </tr> </tbody> </table>	Parameter	Description	<i>probe-count</i>	Number of times that a non-HE radio rejects probe requests from a HIGH-STA, ranging from 0 to 10.
Parameter	Description				
<i>probe-count</i>	Number of times that a non-HE radio rejects probe requests from a HIGH-STA, ranging from 0 to 10.				

**Defaults** 2

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration** The following example sets the number of times that a non-HE radio rejects probe requests from a HIGH-STA to 4.

**Examples** `Hostname(config)# band-select he-radio probe-count 4`

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform** This command is supported on fat APs.

**Description**

## 1.5 show dot11 associations all-client

Use this command to display STA distribution to radios of an AP to display STA distribution of HE radios.

**show dot11 associations all-client** { *radio number* }

Parameter Description	Parameter	Description
	<i>radio number</i>	Number of an RF port.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 15

**Usage Guide** N/A

**Configuration Examples** The following example displays STA distribution to radios of an AP to display STA distribution of HE radios.

```
Hostname# show dot11 associations all-client 1/0
-----
1      3      4      0
2      5      7      0
3#    0      0      8
```

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform Description** This command is supported on fat APs.

# 1 RF Schedule Commands

## 1.1 schedule session

Use this command to configure a scheduling session for a WLAN. Use the **no** form of this command to remove the configuration.

**schedule session** *session-id*


**no schedule session** *session-id*


Parameter Description	Parameter	Description
	<i>session-id</i>	Specifies the ID of the scheduling session to be created or to be applied to a WLAN. The range is from 1 to 64 for an AC and from 1 to 8 for a fat AP.

**Defaults** No scheduling session is configured by default.  
No scheduling session is applied to a WLAN or a radio by default.

**Command mode** Global configuration mode  
WLAN configuration mode  
Dot11radio interface configuration mode.

**Usage Guide** In global configuration mode, you can use this command to create a scheduling session and configure parameters for it. If the scheduling session has been created, the configuration is invalid. On fit AP networking topology, the scheduling session created in WLAN configuration mode will be applied to a WLAN.  
You can specify radio ID or slot ID for the scheduling session. By default, it is applied to all radios instead of slot IDs.

 If you delete the scheduling session in the global configuration mode, the scheduling session on WLAN or Radio is deleted automatically.

 The slot parameter only applies to i-Share + products. This parameter enables auto power-off for Mini AP.

**Configuration Examples** The following example creates or configures scheduling session 1.

```
Hostname(config)# schedule session 1
```

The following example applies scheduling session 1 to WLAN 1

```
Hostname(config)# dot11 wlan 1
```

```
Hostname(dot11-wlan-config)# schedule session 1
```

The following example applies scheduling session 1 to radio 1

```
Hostname(config)# interface dot11radio 1/0
```

```
Hostname(config-if-Dot11radio 1/0)# schedule session 1
```

**Verification** Run the **show running-config** command to view scheduling session configuration and current scheduling session configuration on the WLAN and AP.

Related Commands	Command	Description
	<b>show schedule session</b>	Displays configuration about the scheduling session.
	<b>show running-config</b>	Displays current configuration.

**Platform** N/A

**Description**

## 1.2 schedule session time-range period time

Use this command to set scheduling time for a scheduling session. Use the **no** form of this command to delete the configuration.

**schedule session** *session-id* **time-range** *n* **period** { *day1* [ **to** *day2* ] | **everyday** } **time** { *hh1:mm1* **to** *hh2:mm2* | **all-day** }

**no schedule session** *session-id* **time-range** *n*

Parameter Description	Parameter	Description
	<i>session-id</i>	Specifies the ID of the scheduling session to be created or to be applied to a WLAN. The range is from 1 to 8 for a fat AP.
	<i>n</i>	Specifies the scheduling session time-range ID, in the range from 1 to 8.
	<i>day1</i>	Specifies the start day of the scheduling session time range. Select a value from { Mon, Tue, Wed, Thu, Fri, Sat, Sun }.
	<b>to</b> <i>day2</i>	Specifies the end day of the scheduling session time range. The default scheduling session time range is one day.
	<b>everyday</b>	Specifies that the session occurs every day, which is the simplified form of <b>period</b> <i>sun to sat</i> .
	<b>time</b> <i>hh1:mm1</i> <b>to</b> <i>hh2:mm2</i>	Specifies the start and end time. <i>hh1:mm1</i> indicate the start hour and minute; <i>hh2:mm2</i> indicate the end hour and minute. The hour value is in the range from 0 to 23 and the minute value is in the range from 0 to 59.
	<b>time</b> <b>all-day</b>	Specifies that the session time range is a whole day, which is the simplified form of <b>time</b> <i>00:00 to 23:59</i> .

**Defaults** N/A


**Command** Global configuration mode



**mode**

**Usage Guide** Time range should be specified when you create a scheduling session. One session supports up to 8 time ranges, each of which includes scheduling time and effective date. Same scheduling time and interval take effect in multiple scheduling sessions.

 If *hh2:mm2* is not set, the scheduling time lasts to 23:59 by default.

 If *hh2:mm2* is earlier than *hh1:mm1*, *hh2:mm2* is the time on the next day.

**Configuration Examples** The following example sets the scheduling time of scheduling session 1 to the range from 9:30 pm to 8:50 am on the next day.

```
Hostname(config)# schedule session 1 time-range 1 period sun to sat time 21:30 to 8:50
```

The following example sets the scheduling time of scheduling session 1 to the range from 10:00 pm to 6:00 am on the next day of the working day and from 6:00 pm to 9:00 am on the next day of the weekend.

```
Hostname(config)# schedule session 1 time-range 1 period mon to fri time 22:00 to 6:00
```

```
Hostname(config)# schedule session 1 time-range 2 period sat to sun time 18:00 to 9:00
```

The following example sets the scheduling time of scheduling session 1 to the range from 10:00 am to 12:00 am on Monday, Wednesday and Friday.

```
Hostname(config)# schedule session 1 time-range 1 period mon time 10:00 to 12:00
```

```
Hostname(config)# schedule session 1 time-range 2 period wed time 10:00 to 12:00
```

```
Hostname(config)# schedule session 1 time-range 3 period fri time 10:00 to 12:00
```

**Verification** Run the **show schedule session** command to view the time range configuration of the scheduling session.

Related Commands	Command	Description
	<b>show schedule session</b>	Displays configuration about the scheduling session.

**Platform** N/A

**Description**

### 1.3 show schedule session

Use this command to display configuration about scheduling sessions.

**show schedule session** [ *session-id* ]

Parameter Description	Parameter	Description
	<i>session-id</i>	Specifies a scheduling session ID in the range from 1 to 8

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** If no scheduling session ID is specified, configuration about all scheduling sessions will be displayed.

**Configuration** The following example displays configuration about all scheduling sessions.

**Examples**

```

Hostname# show schedule session
Schedule Session 1:
  time-range 1 period mon time 10:00 to 12:00
  time-range 2 period wed time 10:00 to 12:00
Schedule Session 2:
  time-range 1 period Sun to Sat time 00:00 to 09:00
    
```

Field	Description
Schedule Session	Scheduling session ID
time-range	Time range configuration of the scheduling session
period	Cycle of the scheduling session time range
time	Time period of the scheduling session time range

Related Commands	Command	Description
	<b>schedule session</b>	Configures a scheduling session.

**Platform Description** N/A

# 1 WLAN Location Commands

## 1.1 wlocation ae-ip

Use this command to configure the IP address of the AE server connected with the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation ae-ip** *ip-address*

**no wlocation ae-ip**

### Parameter Description

Parameter	Description
<i>ip-address</i>	The IP address of the AE server

### Defaults

The IP address of the AE server is not configured by default.

### Command

Wlocation configuration mode

### Mode

### Usage Guide

N/A

### Configuration

The following example configures the IP address of the AE server on the specified AP.

### Examples

```
Hostname(config-wlocation)# wlocation ae-ip 1.1.1.1
```

The following example restores the IP address of the AE to the default setting.

```
Hostname(config-wlocation)# no wlocation ae-ip
```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.2 wlocation ae-port

Use this command to set the port number of the AE server connected with the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation ae-port** *port*

**no wlocation ae-port**

### Parameter Description

Parameter	Description
-----------	-------------

<i>port</i>	The port number of the AE server, in the range from 1024 to 65535.
-------------	--

**Defaults** The default port number is 12092.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the port number of the AE server connected with the specified AP.

**Examples**

```
Hostname(config-wlocation)# wlocation ae-port 12093
```

The following example restores the port number of the AE server connected with the specified AP to the default configuration.

```
Hostname(config-wlocation)# no wlocation ae-port
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.3 wlocation compound enable

Use this command to enable the function of transmitting aggregate data of wireless location.

Use the **no** form of this command to disable this function.

**wlocation compound enable**

**no wlocation compound enable**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** This function is enabled by default.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the function of transmitting aggregate data of wireless location on the specified AP.

**Examples**

```
Hostname(config-wlocation)# wlocation compound enable
```

The following example disables the function of transmitting aggregate data of wireless location on the specified AP.

```
Hostname(config-wlocation)# no wlocation compound enable
```

#### Related Commands

Command	Description
N/A	N/A

#### Platform

N/A

#### Description

## 1.4 wlocation enable

Use this command to enable the WLAN Location (WL) function on the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation enable** [ radio *radio-id* ]

**no wlocation enable** [ radio *radio-id* ]

#### Parameter Description

Parameter	Description
N/A	N/A

#### Defaults

This function is disabled by default.

#### Command Mode

Wlocation configuration mode

#### Usage Guide

N/A

#### Configuration Examples

The following example enables WLAN location on the AP.

```
Hostname(config)# wlocation
```

The following example disables WLAN location on the AP.

```
Hostname(config-wlocation)# wlocation enable
```

The following example enables WLAN location on Radio1 of the specified AP.

```
Hostname(config-wlocation)# wlocation enable radio 1
```

The following example disables WLAN location on Radio1 of the specified AP.

```
Hostname(config-wlocation)# no wlocation enable radio 1
```

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.5 wlocation ignore beacon enable

Use this command to enable the AP to ignore beacon packets.

Use the **no** form of this command to restore the default setting.

**wlocation ignore beacon enable**

**no wlocation ignore beacon enable**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** Use this command to ignore beacon packets to save bandwidth.

**Configuration** The following example enables the AP to ignore beacon packets.

**Examples**

```
Hostname(config-wlocation)# wlocation ignore beacon enable
```

The following example disables the AP from ignoring beacon packets.

```
Hostname(config-wlocation)# no wlocation ignore beacon enable
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.6 wlocation mu enable

Use this command to enable Mobile Unit (MU) wireless location on the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation mu enable**

**no wlocation mu enable**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	N/A	N/A

**Defaults** This function is disabled by default.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** MU wireless location locates Wi-Fi connected mobile devices like laptops and mobiles.

**Configuration** The following example enables MU wireless location on the specified AP.

**Examples** `Hostname(config-wlocation)# wlocation mu enable`

The following example disables MU wireless location on the specified AP.

`Hostname(config-wlocation)# no wlocation mu enable`

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Platform** N/A

**Description**

## 1.7 wlocation mu report enable

Use this command to enable the AP to send MU location packets directly.

Use the **no** form of this command to restore the default setting.

**wlocation mu report enable**

**no wlocation mu report enable**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

**Defaults** This function is disabled by default.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** Use this command to send MU location packets directly and travel through NAT network without the three-way handshake.

**Configuration** The following example enables the AP to send MU location packets directly.

**Examples** `Hostname(config-wlocation)# wlocation mu report enable`

The following example disables the AP from sending MU location packets directly.

```
Hostname(config-wlocation)# no wlocation mu report enable
```

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.8 wlocation mu report reduce enable

Use this command to enable the AP to send reduced MU location packets.

Use the **no** form of this command to restore the default setting.

**wlocation mu report reduce enable**

**no wlocation mu report reduce enable**

#### Parameter Description

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

#### Command

**Mode** Wlocation configuration mode

**Usage Guide** Enable the function of simplifying MU location information to reduce bandwidth traffic, which applies only when the location server is developed by Ruijie Networks.

**Configuration** The following example enables the AP to send reduced MU location packets.

**Examples**

```
Hostname(config-wlocation)# wlocation mu report reduce enable
```

The following example disables the AP from sending reduced MU location packets.

```
Hostname(config-wlocation)# no wlocation mu report reduce enable
```

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A  
**Description**



## 1.9 wlocation send-mu-time

Use this command to set frequency of sending MU location packets on the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation send-mu-time** *interval*

**no wlocation send-mu-time**

Parameter Description	Parameter	Description
	<i>interval</i>	Packets sending interval in the range from 100 to 600,000 in the unit of milliseconds.

**Defaults** The default is 300 milliseconds.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** N/A

**Configuration** The following example sets frequency to send MU location packets on the specified AP.

**Examples**

```
Hostname(config)# wlocation
Hostname(config-wlocation)# wlocation send-mu-time 400
```

The following example restores the frequency of sending MU location packets to the default setting.

```
Hostname(config)# wlocation
Hostname(config-wlocation)# no wlocation send-mu-time
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.10 wlocation send-tag-time

Use this command to set frequency to send tag location packets on the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation send-tag-time** *interval*

**no wlocation send-tag-time**

Parameter Description	Parameter	Description
-----------------------	-----------	-------------

<i>interval</i>	Packets sending interval within the range from 100 to 5,000 in the unit of milliseconds.
-----------------	--

**Defaults** The default is 300 milliseconds.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** N/A

**Configuration** The following example sets frequency to send tag location packets on the specified AP.

**Examples**

```
Hostname(config-wlocation)# wlocation send-tag-time 400
```

The following example restores frequency of sending tag location packets to the default setting.

```
Hostname(config-wlocation)# no wlocation send-tag-time
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.11 wlocation tag enable

Use this command to enable tag wireless location on the specified AP.

Use the **no** form of this command to restore the default setting.

**wlocation tag enable**

**no wlocation tag enable**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

**Command**

**Mode** Wlocation configuration mode

**Usage Guide** N/A

**Configuration** The following example enables tag wireless location on the specified AP.

**Examples**

```
Hostname(config-wlocation)# wlocation tag enable
```

The following example disables tag wireless location on the specified AP.

```
Hostname(config-wlocation)# no wlocation tag enable
```

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

## 1.12 wlocation tag report enable

Use this command to enable the function to send TAG location packets directly.

Use the **no** form of this command to restore the default setting.

**wlocation tag report enable**

**no wlocation tag report enable**

#### Parameter Description

Parameter	Description
N/A	N/A

**Defaults** This function is disabled by default.

#### Command

**Mode** Wlocation configuration mode

**Usage Guide** Use this command to send TAG location packets directly and travel through NAT network without the three-way handshake.

**Configuration** The following example enables the AP to send TAG location packets directly.

```
Hostname(config-wlocation)# wlocation tag report enable
```

The following example disables the AP from sending TAG location packets directly.

```
Hostname(config-wlocation)# no wlocation tag report enable
```

#### Related Commands

Command	Description
N/A	N/A

**Platform** N/A  
**Description**



# WLAN Security Commands

---

1. RSNA Commands
2. STA Access Control List Commands
3. WIDS Commands

# 1 RSNA Commands

## 1.1 authtimeout forbidcount

Use this command to configure the forbidcount after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout forbidcount** *count*

**no authtimeout forbidcount**

**default authtimeout forbidcount**

### Parameter Description

Parameter	Description
<i>count</i>	Sets the forbidcount after a four-way handshake fails to accomplish key exchange.

### Defaults

The association is not forbidden after four-way handshake key interaction fails.

### Command mode

WLAN security configuration mode

### Usage Guide

N/A

### Configuration Examples

The following example sets the forbidcount to 5 after a four-way handshake fails to accomplish key exchange.

```
Hostname(config-wlansec)# authtimeout forbidcount 5
```

### Related Commands

Command	Description
N/A	N/A

### Platform

N/A

### Description

## 1.2 authtimeout forbidtime

Use this command to set the forbidtime after a four-way handshake fails to accomplish key exchange. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout forbidtime** *time*

**no authtimeout forbidtime**

**default authtimeout forbidtime**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>time</i></td> <td>Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds.</td> </tr> </tbody> </table>	Parameter	Description	<i>time</i>	Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds.
Parameter	Description				
<i>time</i>	Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds.				
<b>Defaults</b>	The default is 5.				
<b>Command mode</b>	WLAN security configuration mode				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	<p>The following example sets the forbidtime to 6 seconds after a four-way handshake fails to accomplish key exchange,</p> <pre>Hostname(config-wlansec)# authtimeout forbidtime 6</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
<b>Platform Description</b>	N/A				

### 1.3 authtimeout groupcount

Use this command to set the retransmission count for the multicast key agreement packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout groupcount** *count*

**no authtimeout groupcount**

**default authtimeout groupcount**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>count</i></td> <td>Sets the retransmission count for the multicast key negotiation packet.</td> </tr> </tbody> </table>	Parameter	Description	<i>count</i>	Sets the retransmission count for the multicast key negotiation packet.
Parameter	Description				
<i>count</i>	Sets the retransmission count for the multicast key negotiation packet.				
<b>Defaults</b>	The default retransmission count of multicast key negotiation packet is 4.				
<b>Command mode</b>	WLAN security configuration mode				
<b>Usage Guide</b>	N/A				
<b>Configuration</b>	The following example set the retransmission count for the multicast key negotiation packet to 5.				

**Examples** `Hostname(config-wlansec)#authtimeout groupcount 5`

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.4 authtimeout grouptime

Use this command to set the timeout period for the multicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout grouptime** *timeout*

**no authtimeout grouptime**

**default authtimeout grouptime**

Parameter Description	Parameter	Description
	<i>timeout</i>	

**Defaults** The default is 1200 milliseconds.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the timeout period for the multicast key negotiation packet to 100 milliseconds.

`Hostname(config-wlansec)# authtimeout grouptime 100`

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.5 authtimeout paircount

Use this command to set the retransmission count for the unicast key negotiation packet. Use the **no**

or **default** form of this command to restore the default setting.

**authtimeout paircount** *count*

**no authtimeout paircount**

**default authtimeout paircount**

Parameter Description	Parameter	Description
	<i>count</i>	Sets the retransmission count for the unicast key negotiation packet.

**Defaults** The default is 4.

**Command mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the retransmission count for the unicast key negotiation packet to 5.

```
Hostname(config-wlansec)#authtimeout paircount 5
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.6 authtimeout pairtime

Use this command to set the timeout period for the unicast key negotiation packet. Use the **no** or **default** form of this command to restore the default setting.

**authtimeout pairtime** *timeout*

**no authtimeout pairtime**

**default authtimeout pairtime**

Parameter Description	Parameter	Description
	<i>timeout</i>	Sets the timeout period for the unicast key negotiation packet, in the unit of milliseconds.

**Defaults** The default is 1200 milliseconds.

**Command mode** WLAN security configuration mode



**Usage Guide** N/A

**Configuration** The following example sets the timeout period for the unicast key negotiation packet to 100 milliseconds.

**Examples**

```
Hostname(config-wlansec)# authtimeout pairtime 100
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.7 dot1x-mab

Use this command to configure MAB authentication for the specified WLAN. Use the **no** form of this command to restore the default setting.

**dot1x-mab**

**no dot1x-mab**

**Parameter  
Description**

Parameter	Description
<b>no</b>	Clears the MAB authentication configuration.

**Defaults** MAB authentication is disabled by default.

**Command  
mode** WLAN security configuration mode

**Usage Guide** This command is used to enable MAB authentication. It can be used in combination with PSK access authentication but not with 802.1X access authentication.

**Configuration** The following example enables MAB authentication for WLAN 1.

**Examples**

```
Hostname(config)# wlansec 1
```

```
Hostname(config-wlansec)# dot1x-mab
```

The following example disables MAB authentication for WLAN 1.

```
Hostname(config)# wlansec 1
```

```
Hostname(config-wlansec)# no dot1x-mab
```

**Notifications**

When other encryption method such as WEP has been enabled for the WLAN, MAB authentication cannot be enabled, and the following notification will be displayed:  
now, wlan security is other security,please delete the security config first

Common Errors  
Other encryption method such as WEP has been enabled for the WLAN.

Platform N/A  
Description

## 1.8 rsna lazy-response

Use this command to enable response delay for authentication packets.

**rsna lazy-response enable**

Use this command to disable response delay for authentication packets.

**no rsna lazy-response enable**

Use this command to restore the default setting.

**default rsna lazy-response enable**

Use this command to configure the response delay period for authentication packets.

**rsna lazy-response timer** *timer*

Parameter Description

Parameter	Description
<i>timer</i>	Response delay period. The range is 0–2000 ms, and the default value is 1000 ms.

**Defaults** . This function is enabled by default, which is not displayed in the output of the **show run** command.

**Command mode** Global configuration mode.

**Default Level** 14

**Usage Guide** This command is used to enable or disable the response delay function for authentication packets. This function is enabled by default. If auth packets are received when this function is enabled and assoc req packets are being processed within 1000 ms (default value), the newly received auth packets will be discarded and previous packets are still processed. If the processing of assoc req packets has timed out (for example, exceeding 1000 ms), previous assoc req packets are discarded and new auth packets are processed.

**Configuration Examples** The following example disables response delay for authentication packets.

```
Hostname(config)# no rsna lazy-response enable
```

The following example sets the response delay period for authentication packets to

1500 ms.

```
Hostname(config)# rsn lazy-response timer 1500
```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.9 security rsn

Use this command to configure RSN authentication for a WLAN.

**security rsn { enable | disable }**

Use this command to restore the default setting.

**security rsn disable**

Parameter Description	Parameter	Description
	<b>enable</b>	Enables the RSN authentication mode.
	<b>disable</b>	Disables the RSN authentication mode.

**Defaults** This function is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable the RSN authentication mode. Only after the RSN authentication mode is enabled can encryption and authentication methods be configured in the RSN mode. Otherwise, any configuration is invalid. When you use the RSN authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network. The RSN authentication mode is what is usually called WPA2 authentication mode. If both WPA and RSN authentication modes are configured simultaneously for a WLAN, the encryption and authentication methods in these two authentication modes are identical, and the newly configured encryption and authentication methods will override the previous ones.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to RSN.

```
Hostname(config)# wlansec 1
Hostname(config-wlansec)# security rsn enable
```

Related Commands	Command	Description
	<b>security rsn akm { psk   802.1x } { enable   disable }</b>	Configures an authentication method in the RSN authentication mode.
	<b>security rsn ciphers { aes   tkip } { enable   disable }</b>	Configures an encryption method in the RSN authentication mode.
	<b>security rsn akm psk set-key ascii</b>	Configures a shared password for RSNs.

**Platform** N/A

**Description**

## 1.10 security rsn akm

Use this command to set the authentication method for a WLAN in the RSN authentication mode to PSK.

**security rsn akm psk enable**

Use this command to disable the PSK authentication method for a WLAN in the RSN authentication mode.

**security rsn akm psk disable**

Use this command to set the authentication method for a WLAN in the RSN authentication mode to 802.1x authentication.

**security rsn akm 802.1x enable**

Use this command to disable the 802.1x authentication method for a WLAN in the RSN authentication mode.

**security rsn akm 802.1x disable**

Parameter Description	Parameter	Description
	<b>psk</b>	Configures the authentication method to pre-shared key identity verification.
	<b>802.1x</b>	Configures the authentication method to IEEE802.1x authentication.
	<b>enable</b>	Enables an authentication method in the RSN authentication mode.
	<b>disable</b>	Disables an authentication method in the RSN authentication mode.

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an authentication method in the RSN authentication mode. Only after the RSN authentication mode is enabled can an authentication method be configured. There are two authentication methods: PSK and 802.1x.

**Configuration Examples** The following example configures the authentication method for WLAN1 in the RSN authentication mode to PSK.

```
Hostname(config-wlansec)# security rsn akm psk enable
```

The following example sets the authentication method for WLAN1 in the RSN authentication mode to 802.1x authentication.

```
Hostname(config-wlansec)# security rsn akm 802.1x enable
```

**Platform Description** N/A

**Verifications** Run the **show running-config** command to show the configuration.

**Notifications** When RSN authentication is not enabled in the WLAN security configuration mode but an authentication method is enabled for RSN authentication, the following notification will be displayed:

```
Hostname(config)#wlansec 1
Hostname(config-wlansec)#security rsn akm psk enable
WLAN 1 rsn is disable.
```

When an authentication method has been enabled in the WLAN security configuration mode and then another authentication method is enabled, the following notification will be displayed:

```
Hostname(config-wlansec)#security rsn akm psk enable
Hostname(config-wlansec)#security rsn akm 802.1x enable
Wlan 1 has config psk, can not config 1x.
```

**Common Errors** An authentication method is enabled for the RSN authentication mode when RSN authentication is not enabled in the WLAN security configuration mode.  
An authentication method has been enabled in the WLAN security configuration mode.

**Platform Description** -

### 1.11 security rsn akm psk set-key

Use this command to configure a shared password for RSNs in the PSK authentication mode.

```
security rsn akm psk set-key { ascii ascii-key | hex hex-key }
```

Parameter Description	Parameter	Description
	ascii	Specifies the ASCII password.

<i>ascii-key</i>	The ASCII password, containing 8–63 characters.
<b>hex</b>	Specifies the hexadecimal password.
<i>hex-key</i>	The hexadecimal password, containing 64 characters.

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** This shared password is of use only when the PSK authentication mode is enabled.

**Configuration** The following example sets the shared password for WLAN 1 RSN to 12345678.

**Examples**

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)# security rsn enable
Hostname(config-wlansec)# security rsn akm psk enable
Hostname(config-wlansec)# security rsn akm psk set-key ascii 12345678

```

**Verifications** Run the **show running-config** command to show the configuration.

**Notifications** When the length of an ASCII password is less than eight characters, the following notification will be displayed:

```

Hostname(config-wlansec)#security rsn akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).

```

When the length of a hexadecimal password is not 64 characters, the following notification will be displayed:

```

Hostname(config-wlansec)# security rsn akm psk set-key hex
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde

```

Hex PSK length must be 64.

**Common** An RSN PSK password is configured when RSN authentication is not enabled.

**Errors** The length of an ASCII password is less than eight characters or exceeds 63 characters.

The length of a hexadecimal password is not 64 characters.

**Platform Description** N/A

## 1.12 security rsn ciphers

Use this command to set the encryption method for a WLAN in RSN authentication mode to AES.

**security rsn ciphers aes enable**

---

Use this command to disable the AES encryption method for a WLAN in RSN authentication mode.

**security rsn ciphers aes disable**

Use this command to set the encryption method for a WLAN in RSN authentication mode to TKIP.

**security rsn ciphers tkip enable**

Use this command to disable the TKIP encryption method for a WLAN in RSN authentication mode.

**security rsn ciphers tkip disable****Parameter  
Description**

Parameter	Description
<b>aes</b>	Configures the encryption method to AES.
<b>tkip</b>	Configures the encryption method to TKIP.
<b>enable</b>	Enables an encryption method in the RSN authentication mode.
<b>disable</b>	Disables an encryption method in the RSN authentication mode.

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an encryption method in the RSN authentication mode. There are two encryption methods: AES and TKIP.

**Configuration Examples** The following example sets the encryption method for WLAN 1 in RSN authentication mode to AES.

**Examples**

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security rsn enable
Hostname(config-wlansec)#security rsn ciphers aes enable

```

**Verifications** Run the **show running-config** command to show the configuration.

**Notifications** When RSN authentication is not enabled in the WLAN security configuration mode but an encryption method is enabled for RSN authentication, the following notification will be displayed:

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security rsn ciphers aes enable
WLAN 1 rsn is disable.

```

**Common Errors** An encryption method is enabled for the RSN authentication mode when RSN authentication is not enabled in the WLAN security configuration mode.

No encryption method is enabled when RSN authentication is enabled in the WLAN security configuration mode. As a result, STAs cannot associate with the WLAN.

**Platform Description** N/A

## 1.13 security pmf

Use this command to enable or disable management frame encryption.

**security pmf { disable | mandatory | optional }**

Parameter Description	Parameter	Description
	<b>disable</b>	Disables management frame encryption.
	<b>mandatory</b>	Sets management frame encryption to mandatory mode. STAs must support management frame encryption.
	<b>optional</b>	Sets management frame encryption to optional mode. STAs do not need to support management frame encryption.

**Defaults** Management frame encryption is disabled by default.

**Command mode** WLAN security configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration Examples** The following example enables management frame encryption on WLAN 1, with clients required to support this function.

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security rsn enable
Hostname(config-wlansec)#security rsn ciphers aes enable
Hostname(config-wlansec)#security rsn akm psk enable
Hostname(config-wlansec)#security rsn akm psk set-key ascii 12345678
Hostname(config-wlansec)#security pmf mandatory

```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Common Errors**

1. In pure WPA3 mode, PMF needs to be configured as mandatory. Otherwise, terminals cannot access the network.
2. In WPA3 Personal hybrid mode, PMF needs to be configured as optional. The configuration of the WPA3 Personal hybrid mode is WPA2 PSK + pmf optional + WPA3 SAE. In this case, WPA2 PSK terminals and SAE terminals can access the network. If WPA2 PSK + pmf mandatory + WPA3 SAE are configured, the SAE configuration will not take effect and only PMF-supported WPA2 PSK terminals can access the network.



**Platform** N/A  
**Description**

## 1.14 security static-wep-key authentication

Use this command to configure an authentication method for a WLAN in the static WEP mode.

**security static-wep-key authentication** { **open** | **share-key** }

Parameter Description	Parameter	Description
	<b>open</b>	The open system authentication mode.
	<b>share-key</b>	The shared key authentication mode.

**Defaults** The default is **open**.

**Command mode** WLAN security configuration mode

**Usage Guide** This command must be used with the **security static-wep-key encryption** command. Usually, the static WEP key must be configured before the shared key authentication method can be configured. In any security mode other than the static WEP security mode, it is of no use to configure the link authentication mode.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to shared key authentication.

```
Hostname(config-wlansec)# security static-wep-key authentication
share-key
```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** When a link authentication mode is configured if the static WEP mode is not enabled, the following notification will be displayed:

```
Fail to setup WEP authmode, not in static WEP security mode (1).
```

**Common Errors** A link authentication mode is configured when the static WEP mode is not enabled.

**Platform** N/A  
**Description**

## 1.15 security static-wep-key encryption

Use this command to configure the static WEP key for a WLAN and configure the security mode of this WLAN to static WEP.

**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*

Parameter Description	Parameter	Description
	<i>key-length</i>	The key length is measured by bit, which can be 40, 104, and 128 bits.
	<i>key-index</i>	The parameter indicates a key index number, ranging from 1 to 4.
	<i>key</i>	The parameter indicates key data. In the ASCII mode, 5-byte, 13-byte, and 16-byte data can serve as a key depending on the <i>key-length</i> parameter. In the hex mode, 10-byte, 26-byte, and 32-byte data can serve as a key depending on the <i>key-length</i> parameter.
	<b>ascii</b>	The parameter indicates that the password takes the form of ASCII code.
	<b>hex</b>	The parameter indicates that the password is hexadecimal.

**Defaults** The static WEP mode is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** The prerequisite of configuring security mode for a WLAN is that this WLAN has been created. Attention should be paid to the following points:

1. This command can be used repeatedly for configuration, and the last configuration will take effect.
2. This command configures the static WEP key as well as the static-WEP security mode.

**Configuration Examples** The following example sets the static WEP key of WLAN 1 to 12345.

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)# security static-wep-key encryption 40 ascii 1 12345

```

Related Commands	Command	Description
	<b>security static-wep-key authentication { open   share-key }</b>	Configures the authentication method in the static WEP security mode to open system authentication or shared key authentication.

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** When the length of the configured key differs from that of the specified value, the following notification will be displayed:

```

Hostname(config-wlansec)#security static-wep-key encryption 40 ascii 1 123456
password Must be 5 ASCII characters.

```

When the static WEP mode has been configured for an WLAN and then is configured for another WLAN on the device, the following notification will be displayed:

Fail to setup static WEP key, because another wlan has configed static WEP.

**Common Errors** The length of the configured key differs from the specified value.  
The static WEP mode is configured for more than one WLANs.

**Platform Description** N/A

## 1.16 security wpa

Use this command to configure WPA authentication for a WLAN.

**security wpa { enable | disable }**

Parameter Description	Parameter	Description
	<b>enable</b>	Enables WPA authentication.
	<b>disable</b>	Disables WPA authentication.

**Defaults** WPA authentication is disabled by default.

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable the WPA authentication mode. Only after the WPA authentication mode is enabled can encryption and authentication methods be configured in the WPA mode. Otherwise, configuration is impossible. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

**Configuration Examples** The following example sets the authentication mode of WLAN1 to WPA.

```
Hostname(config)# wlansec 1
Hostname(config-wlansec)# security wpa enable
```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** When other encryption method such as WEP has been enabled for the WLAN and then WPA authentication is configured, the following notification will be displayed:  
wlan security is static wep, can't config other security mode

**Common Errors** Other encryption method such as WEP has been enabled for the WLAN.

**Platform Description** N/A

## 1.17 security wpa akm

Use this command to configure the pre-shared key identity authentication for a WLAN in the WPA authentication mode.

**security wpa akm psk enable**

Use this command to disable the pre-shared key identity authentication for a WLAN in the WPA authentication mode.

**security wpa akm psk disable**

Use this command to configure the 802.1x authentication for a WLAN in the WPA authentication mode.

**security wpa akm 802.1x enable**

Use this command to disable the 802.1x authentication for a WLAN in the WPA authentication mode.

**security wpa akm 802.1x disable**

### Parameter Description

Parameter	Description
<b>psk</b>	Configures the authentication method to pre-shared key identity verification.
<b>802.1x</b>	Configures the authentication method to IEEE802.1x authentication.
<b>enable</b>	Enables an authentication method in the WPA authentication mode.
<b>disable</b>	Disables an authentication method in the WPA authentication mode.

### Defaults

N/A

### Command mode

WLAN security configuration mode

### Usage Guide

The command is used to enable an authentication method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an authentication method be configured. There are two authentication methods: PSK and 802.1x. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

### Configuration Examples

The following example sets the authentication method for WLAN1 in the WPA authentication mode to pre-shared key identity authentication.

```
Hostname(config-wlansec)# security wpa akm psk enable
```

The following example sets the authentication method for WLAN1 in the WPA authentication mode to 802.1x authentication.

```
Hostname(config-wlansec)# security wpa akm 802.1x enable
```

**Verifications**

Run the **show running-config** command to check whether the configuration takes effect.

**Notifications**

When WPA authentication is not enabled in the WLAN security configuration mode but an authentication method is enabled for WPA authentication, the following notification will be displayed:

```
Hostname(config)#wlansec 1
Hostname(config-wlansec)#security wpa akm psk enable
WLAN 1 wpa is disable.
```

When an authentication method has been enabled in the WLAN security configuration mode and then another authentication method is enabled, the following notification will be displayed:

```
Hostname(config-wlansec)#security wpa akm psk enable
Hostname(config-wlansec)#security wpa akm 802.1x enable
Wlan 1 has config psk, can not config 1x.
```

**Common Errors**

An authentication method is enabled for the WPA authentication mode when WPA authentication is not enabled in the WLAN security configuration mode.

An authentication method has been enabled in the WLAN security configuration mode.

**Platform****Description**

N/A

## 1.18 security wpa akm psk set-key

Use this command to configure a WPA shared password for a WLAN.

```
security wpa akm psk set-key { ascii ascii-key | hex hex-key }
```

**Parameter  
Description**

Parameter	Description
<b>ascii</b>	Specifies the ASCII password.
<i>ascii-key</i>	The ASCII password, containing 8-63 characters.
<b>hex</b>	Specifies the hexadecimal password.
<i>hex-key</i>	The hexadecimal password, containing 64 characters.

**Defaults**

N/A

**Command mode**

WLAN security configuration mode

**Usage Guide**

This shared password is of use only when the PSK authentication mode is enabled. The length of an ASCII password must range from 8 to 63 characters.

The length of a hexadecimal password must be 64 characters.

**Configuration**

The following example sets the shared password for WLAN 1 WPA to 12345678.

**Examples**

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)# security wpa enable
Hostname(config-wlansec)# security wpa akm psk enable
Hostname(config-wlansec)# security wpa akm psk set-key ascii 12345678
    
```

**Verifications**

Run the **show running-config** command to check whether the configuration takes effect.

**Notifications**

When the length of an ASCII password is less than eight characters, the following notification will be displayed:

```

Hostname(config-wlansec)#security wpa akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).
    
```

When the length of a hexadecimal password is not 64 characters, the following notification will be displayed:

```

Hostname(config-wlansec)# security wpa akm psk set-key hex
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde
Hex PSK length must be 64.
    
```

**Common Errors**

A WPA PSK password is configured when WPA authentication is not enabled.  
 The length of an ASCII password is less than eight characters or exceeds 63 characters.  
 The length of a hexadecimal password is not 64 characters.

**Platform**

N/A

**Description**

## 1.19 security wpa ciphers

Use this command to set the encryption method for a WLAN in WPA authentication mode to AES.

**security wpa ciphers aes enable**

Use this command to disable the AES encryption method for a WLAN in WPA authentication mode.

**security wpa ciphers aes disable**

Use this command to set the encryption method for a WLAN in WPA authentication mode to TKIP.

**security wpa ciphers tkip enable**

Use this command to disable the TKIP encryption method for a WLAN in WPA authentication mode.

**security wpa ciphers tkip disable**

**Parameter Description**

Parameter	Description
-----------	-------------

<b>aes</b>	Configures the encryption method to AES.
<b>tkip</b>	Configures the encryption method to TKIP.
<b>enable</b>	Enables an encryption method in the WPA authentication mode.
<b>disable</b>	Disables an encryption method in the WPA authentication mode.

**Defaults** N/A

**Command mode** WLAN security configuration mode

**Usage Guide** The command is used to enable an encryption method in the WPA authentication mode. Only after the WPA authentication mode is enabled can an encryption method be configured. There are two encryption methods.

Both AES and TKIP can be enabled in the WLAN security configuration mode.

**Configuration Examples** The following example sets the encryption method for WLAN1 in the WPA authentication mode to AES.

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security wpa enable
Hostname(config-wlansec)#security wpa ciphers aes enable

```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** When WPA authentication is not enabled in the WLAN security configuration mode but an encryption method is enabled for WPA authentication, the following notification will be displayed:

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security wpa ciphers aes enable
WLAN 1 wpa is disable.

```

**Common Errors** An encryption method is enabled for the WPA authentication mode when WPA authentication is not enabled in the WLAN security configuration mode.

No encryption method is enabled when WPA authentication is enabled in the WLAN security configuration mode. As a result, STAs cannot associate with the WLAN.

**Platform**

**Description** -

## 1.20 security wpa3 mode

Use this command to set the WPA3 mode.

**security wpa3 mode {enterprise [ccmp-128 | gcmp-256 ] | none | personal }**

**Parameter Description**

Parameter	Description
-----------	-------------

<b>enterprise</b>	Configures WPA3-Enterprise authentication. If <b>ccmp-128</b> or <b>gcmp-256</b> is not configured, the default encryption algorithm GCMP-256 is used.
<b>enterprise ccmp-128</b>	Sets the encryption algorithm of WPA3-Enterprise authentication to CCMP-128.
<b>enterprise gcmp-256</b>	Sets the encryption algorithm of WPA3-Enterprise authentication to GCMP-256.
<b>none</b>	Disables the WPA3 function.
<b>personal</b>	Indicates the WPA3 Personal mode.

**Defaults** WPA3 is disabled by default.

**Command mode** WLAN security configuration mode

**Default Level** 14

- Usage Guide**
- Personal mode: It can be a WPA3 mode or used in combination with the WPA2 PSK mode because it is compatible with WPA2. When it is used jointly with the WPA2 PSK mode, the WPA2 PSK mode does not support TKIP encryption.
  - Enterprise mode: It is the WPA3 Enterprise mode because it is incompatible with WPA2.
  - WPA3 relies on management frame encryption. Management frame encryption must be enabled before WPA3 is enabled.

**Configuration Examples** The following example configures the WPA3 Personal mode for WLAN 1 and sets the password to abcdefgh .

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security pmf optional
Hostname(config-wlansec)#security wpa3 personal passphrase ascii abcdefgh
Hostname(config-wlansec)#security wpa3 mode personal

```

The following example configures the WPA3 Personal mode used in combination with the WPA2 PSK mode for WLAN 1 and sets the password to abc. If an STA associates with an AP via the WPA3 Personal mode, the password is abcdefgh. If the STA associates with the AP via the WPA2 PSK mode, the password is 123456789.

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security pmf optional
Hostname(config-wlansec)#security wpa3 personal passphrase ascii abcdefgh
Hostname(config-wlansec)#security wpa3 mode personal
Hostname(config-wlansec)#security rsn enable
Hostname(config-wlansec)#security rsn cipher aes enable
Hostname(config-wlansec)#security rsn akm psk enable
Hostname(config-wlansec)#security rsn akm psk set-key ascii 123456789

```

The following example configures the WPA3 Enterprise mode for WLAN 1.

```

Hostname(config)#wlansec 1

```



```

Hostname(config-wlansec)#security pmf optional
Hostname(config-wlansec)#security wpa3 mode enterprise gcmp-256

```

The following example configures the WPA3 Enhanced-Open mode for WLAN 1.

```

Hostname(config)#wlansec 1
Hostname(config-wlansec)#security pmf optional
Hostname(config-wlansec)#security wpa3 mode enterprise ccmp-128

```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.21 security wpa3 personal passphrase

Use this command to configure a password for the WPA3 Personal mode.

**security wpa3 personal passphrase { none / ascii password }**

Parameter Description	Parameter	Description
	<i>password</i>	Indicates a password in ASCII code, consisting of 1 to 63 characters.
	<b>none</b>	Clears the password.

**Defaults** No password is configured for the WPA3 Personal mode.

**Command mode** WLAN security configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure a password for the WPA3 Personal mode. In WPA3 Personal mode, this password is used in the negotiation between APs and STAs. When the WPA3 Personal mode is used in combination with the WPA2 PSK mode, if an STA supports WPA3, this password is used; if it does not support WPA3, the WPA2 PSK password is used.

**Configuration Examples** The following example sets the password to abcdefgh for the WPA3 personal mode for WLAN 1.

```

Hostname(config)#wlansec 1

```

```
Hostname(config-wlansec)#security wpa3 personal passphrase ascii abcdefgh
```

**Verifications** Run the **show running-config** command to check whether the configuration takes effect.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.22 show wclient security

Use this command to display security configuration of STAs.

**show wclient security** *mac-address*

Parameter Description	Parameter	Description
	<i>mac-address</i>	The MAC address of the STA to be displayed.

**Defaults** N/A

**Command mode** Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the security configuration of wireless client 1 with a MAC address of 3848.4c48.d953.

```
Hostname# show wclient security 3848.4c48.d953
Security policy finished      :TRUE
Security policy type         :PSK
Security WPA version         :WPA2
Security Ucast cipher        :CCMP
Security EAP type            :NONE
```

Field	Description
Security policy finished	Whether the authentication is complete.
Security policy type	Security policy type.
Security WPA version	WPA version.
Security Ucast cipher	Unicast cipher suite

Security EAP type	EAP Type
-------------------	----------

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.23 show wlan security

Use this command to display security configuration of a WLAN.

**show wlan security** *wlan-id*

Parameter Description	Parameter	Description
	<i>wlan-id</i>	The ID of the WLAN to be checked, in the range from 1 to 512.

**Defaults** N/A

**Command mode** Privileged EXEC mode/Global configuration mode/WLAN security configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the security configuration of WLAN 1.

### Examples

```

Hostname# show wlan security 1
WLAN SSID          : autowifi_ef5a
Security Policy    : PSK
WPA version        : RSN(WPA2)
SAE                 : False
802.1X             : False
PSK                 : True
pairwise cipher type: NONE (no cipher)
group cipher type  : NONE (no cipher)
wpa_passhraselen   : 8
wpa_passphrase     : 31 32 33 34 35 36 37 38
group key           :
GN_igtk/GM_igtk    : 0/0
igtk                : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ieee80211w         : disabled
ieee80211r         : 802.11r disabled

```

The following example displays the security configuration of WLAN 2. The WPA3 Enterprise 192-bit

mode is used.

```

Hostname#show wlan security 2
WLAN SSID          : WPA3-ENTERPRISE-DEMO
Security Policy    : 802.1X-WPA3
WPA version        : WPA3
SAE                : False
802.1X            : True
PSK                : False
pairwise cipher type: GCMP256
group cipher type  : GCMP256
wpa_passhraselen  : 0
wpa_passphrase     :
sae_passhraselen  : 0
sae_passphrase     :
group key          : 8c cd b3 84 8f 33 a4 2d 51 73 02 94 1c da 34 c6 19 68 1e 8a 60 aa aa
                   0e 16 ec 89 9f 3f d1 9b fe

```

The following example displays the security configuration of WLAN 2. The WPA3 Enterprise-Only mode is used.

```

Hostname#show wlan security 2
WLAN SSID          : WPA3-ENTERPRISE-CCMP-128
Security Policy    : 802.1X-WPA3-CCMP-128
WPA version        : WPA3
SAE                : False
802.1X            : True
PSK                : False
pairwise cipher type: AES
group cipher type  : AES
wpa_passhraselen  : 0
wpa_passphrase     :
sae_passhraselen  : 0
sae_passphrase     :
group key          : bc 31 b6 ac cd 0a e8 29 33 d3 9e a2 d8 b3 7d 09

```

Field	Description
WLAN SSID	WLAN SSID
Security Policy	Security policy, which can be set to any of the following values: <ul style="list-style-type: none"> <li>SAE: Indicates the WPA3 Personal mode.</li> <li>SAE/PSK: Indicates the WPA3 Personal and WPA2 PSK hybrid mode.</li> <li>802.1X-WPA3: Indicates the WPA3 Enterprise mode.</li> <li>802.1X-WPA3-CCMP-128: WPA3 Enterprise-Only mode</li> </ul>
WPA version	WPA version.
AKM type	AKM suite, indicating the authentication mode.
pairwise cipher type	Unicast cipher suite.

group cipher type	Multicast cipher suite.
wpa_passphrase_len	Password length.
wpa_passphrase	PSK password.
group key	Multicast key.

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.24 wlansec

Use this command to configure security configuration mode for the specified WLAN. Use the **no** or **default** form of this command to restore the default setting.

- wlansec** *wlan-id*
- no wlansec** *wlan-id*
- default wlansec** *wlan-id*

Parameter Description	Parameter	Description
	<i>wlan-id</i>	

**Defaults** No WLAN security configuration mode is configured by default.

**Command mode** Global configuration mode

**Usage Guide** Create a WLAN before entering its security configuration mode. You can use the **no wlansec** *wlan-id* command to clear the WLAN security configuration.

**Configuration Examples** The following example configures security configuration mode for WLAN 1.

```
Hostname(config)# wlansec 1
```

**Verifications** Run the **show wlan security 1** command to check whether the security configuration mode is configured for WLAN 1.

**Notifications** When the WLAN for which security configuration mode needs to be configured does not exist, the following notification will be displayed:

```
Hostname(config)#wlansec 2
Hostname(config)#No wlan or no ssid for this wlanid(2).
```

**Not**

**Common  
Errors**

---

The WLAN for which security configuration mode needs to be configured does not exist.

---

**Platform  
Description**

---

N/A

---

# 1 STA Access Control List Commands

## 1.1 blacklist mac

Use this command to add an STA to the blacklist of an access point (AP) or service set identifier (SSID).

A mnemonic is used to identify the identity of an STA to facilitate reading.

Use the **no** form of this command to delete an STA.

**blacklist mac** *sta-mac* [ **in-ssid** *ssid-string* ] [ **mnemonic** *string* ]

**no blacklist mac** *sta-mac* [ **in-ssid** *ssid-string* ]

Parameter	Parameter	Description
Description	<i>sta-mac</i>	Media access control (MAC) address of an STA. If no parameter is carried after the MAC address, a blacklist is configured for the entire device.
	<b>in-ssid</b> <i>ssid-string</i>	Configures a blacklist for an SSID. After the blacklist is configured, STAs in the blacklist cannot associate with the SSID.
	<i>string</i>	Mnemonic, which is displayed in the output of the <b>show</b> command to facilitate reading.

**Defaults** No STA is added to the blacklist by default.

**Command Mode** STA access control list configuration mode

**Default Level** 15

- Usage Guide**
- After a blacklist is configured, STAs that meet the conditions are not allowed to access the network.
  - Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs.
  - The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
  - Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types.
  - When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately.
  - In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

**Configuration** The following example adds an STA to the MAC address blacklist of the AP.

**Examples**

```
Hostname(config)# black-white-list
```

```
Hostname(black-white-list)# blacklist mac 0025.9cb3.fd2c mnemonic test
```

The following example deletes an STA from the MAC address blacklist of the AP.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#no blacklist mac 0025.9cb3.fd2c
```

**Verification** Run the **show black-white-list blacklist [in-ap *ap-mac* | in-ssid *ssid-string*]** command to display the STAs added to the blacklist.

**Prompts** N/A

**Common Errors**

**Platform** This command is supported on ACs and fat APs.

**Description**

## 1.2 blacklist vendor mac

**Function** Use this command to add an STA to an organizationally unique identifier (OUI) blacklist.

**Command** Use this command to add an STA to the OUI blacklist of an AP or SSID in STA access control list configuration mode.

Use the **no** form of this command to delete an STA from the OUI blacklist of an AP or SSID in STA access control list configuration mode.

**blacklist vendor mac *sta-oui* [ in-ssid *ssid-string* ] [ mnemonic *string* ]**

**no blacklist vendor mac *sta-oui* [in-ssid *ssid-string*]**

]

**Parameter Description**

Parameter	Description
<i>sta-oui</i>	OUI of an STA, in the format of hhhh.hh. If there are no parameters after <b>sta-oui</b> , a blacklist is configured for the entire device.
<b>in-ssid</b> <i>ssid-string</i>	Configures an OUI blacklist for an SSID.
<i>string</i>	Mnemonic, which is displayed in the output of the <b>show</b> command to facilitate reading.

**Defaults** No STA is added to the OUI blacklist by default.

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide**

- The OUI blacklist is used to match OUIs of STAs. STAs of vendors in the OUI blacklist are not



allowed to access the network.

- Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs.
- The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
- Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types.
- When the blacklist is enabled, an online STA that meet the conditions will be kicked offline immediately.
- In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

**Configuration** The following example adds an STA to the OUI blacklist of the AP.

**Examples**

```

Hostname (config) # black-white-list
Hostname (black-white-list) #blacklist vendor mac 0025.9c mnemonic test
    
```

The following example deletes an STA from the OUI blacklist of the AP.

```

Hostname (config) # black-white-list
Hostname (black-white-list) #no blacklist vendor mac 0025.9c
    
```

**Verification** Run the **show black-white-list blacklist [ vendor ] [ in-ssid ssid-string]** command to display the STAs added to the blacklist.

**Prompts** N/A

**Common Errors**

**Platform** This command is supported on fat APs.

**Description**

### 1.3 black-white-list

Use this command to enter the STA access control list configuration mode.

**black-white-list**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration** The following example enters the STA access control list configuration mode.

**Examples**

```

Hostname (config) # black-white-list
Hostname (black-white-list) #

```

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform** This command is supported on fat APs.

**Description**

## 1.4 export

Use this command to export the STA access control list configuration to a file.

**export**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide** This command is used to export the current configuration to the **black-white-list.csv** file in the **/data/** directory.

**Configuration** The following example exports the configuration to the **black-white-list.csv** file.

**Examples**

```

Hostname (config) # black-white-list
Hostname (black-white-list) # export

```

**Verification** Run the **dir** command to display the exported file. Run the **more** command to display the content of the file.

<b>Prompts</b>	Number of entries exported successfully
<b>Common Errors</b>	The flash memory is insufficient to save the exported configuration file, and a prompt is printed.
<b>Platform Description</b>	This command is supported on ACs and fat APs.

## 1.5 import

Use this command to import the STA access control list configuration from a file.

```
import filename { replace | append }
```

Parameter Description	Parameter	Description
	<i>filename</i>	Name of the file to be imported. The file name can contain a path. The default path is <b>/data/</b> .
	<b>replace</b>	Uses the imported configuration to overwrite the current configuration.
	<b>append</b>	Appends the imported configuration to the current configuration.

**Defaults** N/A

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide** If you select **replace**, the imported configuration will overwrite the current configuration.  
If you select **append**, the imported configuration will be appended to the current configuration.

**Configuration Examples** The following example imports the configuration from the **black-white-list.csv** file to overwrite the current configuration.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#import black-white-list replace
```

The following example imports the configuration from the **black-white-list.csv** file and appends it to the current configuration.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#import black-white-list append
```

**Verification** Run the **show black-white-list config** command to display the configurations.

**Prompts** N/A

**Common** N/A  
**Errors**

**Platform** This command is supported on ACs and fat APs.  
**Description**

## 1.6 reset blacklist

Use this command to clear entries in the blacklist of an AP or SSID.

**reset blacklist [ vendor ] [in-ssid ssid-string ]**

Parameter Description	Parameter	Description
	N/A	If there are no parameters after <b>reset blacklist</b> , entries in the blacklist of the AP are cleared.
	<b>vendor</b>	Clears entries in an OUI blacklist.
	<b>in-ssid</b> <i>ssid-string</i>	Clears entries in the blacklist of an SSID.

**Defaults** N/A

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration** The following example clears entries in the MAC address blacklist of the AP.

### Examples

```
Hostname(config)# black-white-list
Hostname(black-white-list)#reset blacklist
```

The following example clears entries in the OUI blacklist of the AP.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#reset blacklist vendor
```

**Verification** Run the **show black-white-list black [vendor] [in-ssid ssid-string]** command to display the STAs added to the blacklist.

**Prompts** N/A

**Common** N/A  
**Errors**

**Platform** This command is supported on ACs and fat APs.  
**Description**

## 1.7 reset whitelist

Use this command to clear entries in the whitelist of an AP or SSID.

**reset whitelist** [ vendor ] [ in-ssid *ssid-string* ]

Parameter Description	Parameter	Description
	N/A	If there are no parameters after <b>reset whitelist</b> , entries in the whitelist of the AP are cleared.
	<b>vendor</b>	Clears entries in an OUI whitelist.
	<b>in-ssid</b> <i>ssid-string</i>	Clears entries in the whitelist of an SSID.

**Defaults** N/A

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide** N/A

**Configuration Examples** The following example clears entries in the MAC address whitelist of the AP.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#reset whitelist
```

The following example clears entries in the OUI whitelist of the AP.

```
Hostname(config)# black-white-list
Hostname(black-white-list)#reset whitelist vendor
```

**Verification** Run the **show black-white-list white** [vendor] [ in-ssid *ssid-string* ] command to display the STAs added to the whitelist.

**Prompts** N/A

**Common Errors** N/A

**Platform Description** This command is supported on fat APs.

## 1.8 show black-white-list

Use this command to display the status and configuration of the STA access control blacklist/whitelist.

**show black-white-list** { summary | config | conflict | sta-mac *sta-mac* | blacklist [vendor] [in-ssid

*ssid-string* ] | **whitelist** [ **vendor** ] [in-ssid *ssid-string* ] }

Parameter Description	Parameter	Description
	<b>summary</b>	Displays basic information about the STA access control list, such as the enabling status and number of entries.
	<b>config</b>	Displays the complete configuration of the STA access control list.
	<b>conflict</b>	Displays STAs in both the blacklist and whitelist.
	<b>sta-mac</b> <i>sta-mac</i>	Displays the blacklist/whitelist configuration type of a specific STA.
	<b>blacklist</b>	Displays entries and mnemonics in the MAC address blacklist of the AP.
	<b>blacklist vendor</b>	Displays entries and mnemonics in the OUI blacklist of the AP.
	<b>blacklist in-ssid</b> <i>ssid-string</i>	Displays entries and mnemonics in the MAC address blacklist of an SSID.
	<b>blacklist vendor in-ssid</b> <i>ssid-string</i>	Displays entries and mnemonics in the OUI blacklist of an SSID.
	<b>whitelist</b>	Displays entries and mnemonics in the MAC address whitelist of the AP.
	<b>whitelist vendor</b>	Displays entries and mnemonics in the OUI whitelist of the AP.
	<b>whitelist in-ssid</b> <i>ssid-string</i>	Displays entries and mnemonics in the MAC address whitelist of an SSID.
	<b>whitelist vendor in-ssid</b> <i>ssid-string</i>	Displays entries and mnemonics in the OUI whitelist of an SSID.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 15

**Usage Guide** N/A

**Configuration** The following example displays the complete STA access control list configuration.

**Examples**

```

Hostname (config) # black-white-list
Hostname (black-white-list) #show black-white-list config

```

**Verification** N/A

**Prompts** N/A

**Common Errors** N/A

**Platform** This command is supported on fat APs.

**Description**

## 1.9 whitelist mac

Use this command to add an STA to the whitelist of an AP or SSID. A mnemonic is used to identify the identity of an STA to facilitate reading.

Use the **no** form of this command to delete an STA.

**whitelist mac** *sta-mac* [**in-ssid** *ssid-string*] [**mnemonic** *string*]

**no whitelist mac** *sta-mac* [**in-ssid** *ssid-string*]

Parameter	Parameter	Description
Description	<i>sta-mac</i>	MAC address of an STA. If there are no parameters after <b>sta-mac</b> , a whitelist is configured for the entire device.
	<b>in-ssid</b> <i>ssid-string</i>	Configures a whitelist for an SSID.
	<i>string</i>	Mnemonic, which is displayed in the output of the <b>show</b> command to facilitate reading.

**Defaults** No STA is added to the whitelist by default.

**Command Mode** STA access control list configuration mode

**Mode**

**Default Level** 15

- Usage Guide**
- After a whitelist is configured, only STAs that meet conditions are allowed to access the network.
  - If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network.
  - Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs.
  - The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
  - Blacklist has a higher priority than whitelist. For example, an STA added to any type of blacklist (MAC address/OUI blacklist of an AP or SSID) cannot go online even if it is added to whitelists of other types.
  - When an entry is added to the whitelist, other STAs will not be kicked offline.
  - In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

**Configuration** The following example adds an STA to the MAC address whitelist of the AP.

**Examples**

```

Hostname(config)# black-white-list
Hostname(black-white-list)# whitelist mac 0025.9cb3.fd2c mnemonic test

```

The following example deletes an STA from the MAC address whitelist of the AP.

```

Hostname(config)# black-white-list
Hostname(black-white-list)# no whitelist mac 0025.9cb3.fd2c

```

**Verification** Run the **show black-white-list whitelist [in-ssid ssid-string]** command to display the STAs added to the whitelist.

**Prompts** N/A

**Common Errors**

**Platform** This command is supported on fat APs.

**Description**

## 1.10 whitelist vendor mac

**Function** Use this command to add an STA to an OUI whitelist.

**Command** Use this command to add an STA to the OUI whitelist of an AP or SSID in STA access control list configuration mode.

Use the **no** form of this command to delete an STA from the OUI whitelist of an AP or SSID in STA access control list configuration mode.

**whitelist vendor mac** *sta-oui* [ **in-ssid** *ssid-string*] [**mnemonic** *string*]

**no whitelist vendor mac** *sta-oui* [ **in-ssid** *ssid-string*]

Parameter Description	Parameter	Description
	<i>sta-oui</i>	OUI of an STA, in the format of hhhh.hh. If there are no parameters after <b>sta-oui</b> , a whitelist is configured for the entire device.
	<b>in-ssid</b> <i>ssid-string</i>	Configures an OUI whitelist for an SSID.
	<i>string</i>	Mnemonic, which is displayed in the output of the <b>show</b> command to facilitate reading.

**Defaults** No STA is added to the OUI whitelist by default.

**Command Mode** STA access control list configuration mode

**Default Level** 15

**Usage Guide**

- The OUI whitelist is used to match the OUIs of STAs. STAs of vendors in the OUI whitelist are allowed to access the network.



- If the whitelist is empty, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network.
- Different types of blacklists and whitelists are complex in priority. You are advised to select a single type according to your needs.
- The MAC address whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
- When an entry is added to the whitelist, other STAs will not be kicked offline.
- In STA access control list configuration mode, run the **show black-white-list config** command to display the blacklist and whitelist configurations.

**Configuration** The following example adds an STA to the OUI whitelist of the AP.

**Examples**

```
Hostname(config)# black-white-list
Hostname(black-white-list)# whitelist vendor mac 0025.9c mnemonic test
```

The following example deletes an STA from the OUI whitelist of the AP.

```
Hostname(config)# black-white-list
Hostname(black-white-list)# no whitelist vendor mac 0025.9c
```

**Verification** Run the **show black-white-list whitelist [vendor] [in-ssid ssid-string]** command to display the STAs added to the whitelist.

**Prompts** N/A

**Common**

**Errors**

**Platform** This command is supported on fat APs.

**Description**

# 1 WIDS Commands

## 1.1 attack-detection enable

Use this command to enable the IDS attack detection. Use the **no** form of this command to restore the default setting.

**attack-detection enable** { all | flood | ddos | spoof | weak-iv }

**no attack-detection enable** { all | flood | ddos | spoof | weak-iv }

Parameter Description	Parameter	Description
	<b>all</b>	Enables all types of IDS attack detection.
	<b>flood</b>	Enables the Flooding IDS attack detection.
	<b>weak-iv</b>	Enables the Weak-IV IDS attack detection.
	<b>spoof</b>	Enables the Spoofing IDS attack detection.
	<b>ddos</b>	Enables the DDOS IDS attack detection.

**Defaults** This function is disabled by default.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the Flooding IDS attack detection.

**Examples**

```
Hostname(config-wids)# attack-detection enable flood
```

The following example disables the Flooding IDS attack detection.

```
Hostname(config-wids)# no attack-detection enable flood
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.2 attack-detection ddos

Use this command to specify the packet threshold and interval for DDOS attack detection. Use the **no** form of this command to restore the default setting.

**attack-detection ddos** { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }  
**no attack-detection ddos** { **arp-threshold** | **icmp-threshold** | **syn-threshold** | **interval** }

Parameter Description	Parameter	Description
	<b>interval</b> <i>time</i>	DDOS detection interval in the range from 10 to 60 in the unit of seconds.
	<b>arp-threshold</b> <i>num</i>	ARP packet threshold in the range from 1 to 10000 in the unit of pps.
	<b>icmp-threshold</b> <i>num</i>	ICMP packet threshold in the range from 1 to 10000 in the unit of pps.
	<b>syn-threshold</b> <i>num</i>	SYN packet threshold in the range from 1 to 10000 in the unit of pps.

**Defaults** The **arp-threshold** is 50pps, **icmp-threshold** is 100pps, **syn-threshold** is 50pps, and **interval** is 30 seconds by default.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets ARP packet threshold to 200pps for DDOS attack detection.

```
Hostname(config-wids)# attack-detection ddos arp-threshold 200
```

The following example restores ARP packet threshold to the default setting.

```
Hostname(config-wids)# no attack-detection ddos arp-threshold
```

**Platform Description** N/A

### 1.3 attack-detection flood multi-mac

Use this command to specify the packet threshold and interval for flooding attack detection in a multi-user system. Use the **no** form of this command to restore the default setting.

**attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *threshold-num* **interval** *interval-time*  
**no attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** }

Parameter Description	Parameter	Description
	<b>assoc</b>	Specifies the association packet.
	<b>reassoc</b>	Specifies the reassociation packet.
	<b>disassoc</b>	Specifies the disassociation packet.
	<b>probe</b>	Specifies the probe request packet.
	<b>action</b>	Specifies the action packet.

<b>auth</b>	Specifies the authentication packet.
<b>deauth</b>	Specifies the deauthentication packet.
<b>null-data</b>	Specifies the null data packet.
<i>threshold-num</i>	Packet threshold in the range from 1 to 10,000.
<i>interval-time</i>	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

**Defaults** The **threshold** is 4,800 and the **interval** is 10 seconds by default.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets **assoc** to 200 and **interval** to 20s for Flooding attack detection in a multi-user system.

```
Hostname(config-wids)# attack-detection flood multi-mac assoc threshold 200
interval 20
```

The following example restores **assoc** and **interval** to the default setting.

```
Hostname(config-wids)#no attack-detection flood multi-mac assoc
```

**Platform Description** N/A

### 1.4 attack-detection flood single-mac

Use this command to set the packet threshold and statistics interval for Flooding attack detection in a single-user system. Use the **no** form of this command to restore the default setting.

**attack-detection flood single-mac { total | assoc | reassoc | disassoc | probe | action | auth | deauth | null-data } threshold *threshold-num* interval *interval-time***  
**no attack-detection flood single-mac { tota | assoc | reassoc | disassoc | probe | action | auth | deauth | null-data }**

Parameter Description	Parameter	Description
	<b>total</b>	Specifies all types of packets.
	<b>assoc</b>	Specifies the association packet.
	<b>reassoc</b>	Specifies the reassociation packet.
	<b>disassoc</b>	Specifies the disassociation packet.
	<b>probe</b>	Specifies the probe request packet.
	<b>action</b>	Specifies the action packet.
	<b>auth</b>	Specifies the authentication packet.

<b>deauth</b>	Specifies the deauthentication packet.
<b>null-data</b>	Specifies the null data packet
<i>threshold-num</i>	Packet threshold in the range from 1 to 5000.
<i>interval-time</i>	Statistics interval threshold in the range from 10 to 60 in the unit of seconds.

**Defaults** The **threshold** is 300 and the **interval** is 10 seconds by default.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example sets **assoc** to 200 and **interval** to 60 seconds for Flooding attack detection in a single-user system.

```
Hostname(config-wids)# attack-detection flood single-mac assoc threshold 200
interval 60
```

The following example restores **assoc** and **interval** to the default setting.

```
Hostname(config-wids)# no attack-detection flood single-mac assoc
```

**Platform Description** N/A

## 1.5 attack-detection spoof

Use this command to set the packet threshold and statistics interval for Spoofing attack detection. Use the **no** form of this command to restore the default setting.

**attack-detection spoof { threshold *threshold-num* | interval *interval-time* }**

**no attack-detection spoof { threshold | interval }**

Parameter Description	Parameter	Description
	<i>threshold-num</i>	Packet threshold in the range from 1 to 1000.
	<i>interval-time</i>	Detection interval in the range from 1 to 60 in the unit of seconds.

**Defaults** The **threshold** is 1 second and the **interval** is 50 seconds by default.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the packet threshold for Spoofing attack detection to 20.

**Examples** `Hostname (config-wids) # attack-detection spoof threshold 20`

The following example restores the ARP packet threshold for Spoofing attack detection to the default setting.

`Hostname (config-wids) # no attack-detection spoof threshold`

**Platform** N/A  
**Description**

## 1.6 attack-detection weak-iv

Use this command to set the packet threshold and interval for Weak IV attack. Use the **no** form of this command to restore the default setting.

**attack-detection weak-iv** { **threshold** *num* | **interval** *time* }

**no attack-detection weak-iv** { **threshold** | **interval** }

Parameter	Parameter	Description
<b>Description</b>	<b>threshold</b> <i>num</i>	Packet threshold in the range from 1 to 10000.
	<b>interval</b> <i>time</i>	Detection interval in the range from 1 to 60 in the unit of seconds.

**Defaults** The **threshold** is 10 seconds and the **interval** is 15 seconds by default.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the packet threshold for Weak IV attack detection to 200.

**Examples** `Hostname (config-wids) # attack-detection weak-iv threshold 200`

The following example restores the packet threshold for Weak IV attack to the default setting.

`Hostname (config-wids) # no attack-detection weak-iv threshold`

**Platform** N/A  
**Description**

## 1.7 attack-detection statistics ap-max

Use this command to configure the maximum number of IDS attack detection lists on the AP. Use the **no** form of this command to restore the default setting.

**attack-detection statistics ap-max** *num*

**no attack-detection statistics ap-max**

Parameter	Parameter	Description
Description	<i>num</i>	The maximum number of IDS attack detection lists on the AP in the range from 1 to 1024.
Defaults	The default is 512.	
Command	WIDS configuration mode	
Mode		
Usage Guide	N/A	
Configuration	The following example sets the maximum number of IDS attack detection lists on the AC to 1000.	
Examples	<pre>Hostname(config-wids)# attack-detection statistics ap-max 1000</pre>	
	The following example restores the maximum number of IDS attack detection lists to the default setting.	
	<pre>Hostname(config-wids)#no attack-detection statistics ap-max</pre>	
Platform	N/A	
Description		

## 1.8 countermeasures ap-max

Use this command to configure the maximum number of APs for the countermeasures.

Use the **no** form of this command to restore the default setting.

**countermeasures ap-max** *ap-num*

**no countermeasures ap-max**

Parameter	Parameter	Description
Description	<i>ap-num</i>	Specifies the maximum number of APs for the countermeasures in the range from 1 to 256.
Defaults	The default is 30.	
Command	WIDS configuration mode	
Mode		
Usage Guide	N/A	
Configuration	The following example sets the maximum number of APs for the countermeasures to 22.	
Examples	<pre>Hostname(config-wids)# countermeasures ap-max 22</pre>	
	The following example restores the maximum number of APs for the countermeasures to the default setting.	

```
Hostname (config-wids) # no countermeasures ap-max
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.9 countermeasures enable

Use this command to enable the device countermeasures. Use the **no** form of this command to restore the default setting.

- countermeasures enable**
- no countermeasure enable**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** WIDS configuration mode

**Usage Guide** This command does not take effect in AP normal working mode.

**Configuration Examples** The following example enables the device countermeasures.

```
Hostname (config-wids) # countermeasures enable
```

The following example disables the device countermeasures.

```
Hostname (config-wids) # no countermeasures enable
```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.10 countermeasures channel-match

Use this command to enable the channel-based countermeasures. Use the **no** form of this command to



restore the default setting.  
**countermeasures channel-match**  
**no countermeasures channel-match**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** WIDS configuration mode

**Usage Guide** Use this command after the device countermeasures are enabled.

**Configuration Examples** The following example enables the channel-based countermeasures.

```
Hostname(config-wids)# countermeasures channel-match
```

The following example disables the channel-based countermeasures.

```
Hostname(config-wids)# no countermeasures channel-match
```

**Platform Description** N/A

### 1.11 countermeasures interval

Use this command to set the device countermeasures interval. Use the **no** form of this command to restore the default setting.

**countermeasures interval *time***  
**no countermeasures interval**

Parameter	Parameter	Description
Description	<i>time</i>	Device countermeasures interval in the range from 100 to 10000 in the unit of milliseconds.

**Defaults** The default is 1000 milliseconds.

**Command Mode** WIDS configuration mode

**Usage Guide** The containment function has no effect when the AP operates in Normal mode.

**Configuration** The following example sets the countermeasures interval to 2000 milliseconds.

**Examples** `Hostname (config-wids) # countermeasures interval 2000`

The following example restores the countermeasures interval to the default setting.

`Hostname (config-wids) # no countermeasures interval`

**Platform** N/A  
**Description**

## 1.12 countermeasures mode

Use this command to configure the device countermeasures mode. Use the **no** form of this command to restore the default setting.

**countermeasures mode** { all | adhoc | config | rogue | ssid }  
**no countermeasures mode** { all | adhoc | config | rogue | ssid }

Parameter Description	Parameter	Description
	<b>all</b>	Indicates all countermeasures are enabled.
	<b>ssid</b>	Indicates the devices with the same SSID on the device are subjected to the countermeasures.
	<b>rogue</b>	Indicates only detected rogue devices are subjected to the countermeasures.
	<b>adhoc</b>	Indicates only detected adhoc devices are subjected to the countermeasures.
	<b>config</b>	Indicates only the devices configured in the static attack list are subjected to the countermeasures.

**Defaults** This function is disabled by default.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** The containment function has no effect when the device operates in Normal mode.

**Configuration** The following example sets the device countermeasures mode to **adhoc**.

**Examples** `Hostname (config-wids) # countermeasure mode adhoc`

The following example disables the **adhoc** mode.

`Hostname (config-wids) # no countermeasures mode adhoc`

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.13 countermeasures rssi-min

Use this command to configure the lower limit of the signal for the countermeasures.

Use the **no** form of this command to restore the default setting.

**countermeasures rssi-min num**

**no countermeasures rssi-min**

Parameter	Parameter	Description
Description	<i>num</i>	Specifies the lower limit of the signal strength for the countermeasures in the range from 0 to 75 (-95 to -20).

**Defaults** The default is 25 (-70).

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the lower limit of the signal strength for the countermeasures to 40.

```
Hostname(config-wids)# countermeasures rssi-min 40
```

The following example restores the default setting.

```
Hostname(config-wids)# no countermeasures rssi-min
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.14 countermeasures fuzzy-enable

Use this command to enable the fuzzy containment function.

Use the **no** form of this command to disable this function.

**countermeasures fuzzy-enable**

**no countermeasures fuzzy-enable**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	N/A	N/A

**Defaults** By default, fuzzy containment is disabled.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** If containment modes include the configuration containment mode, rogue APs whose SSID are similar to those in the SSID blacklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local host are contained. Fuzzy containment takes effect only in configuration containment mode and SSID containment mode.

**Configuration** The following example enables the fuzzy containment function.

**Examples**

```
Hostname(config-wids)# countermeasures fuzzy-enable
```

The following example disables the fuzzy containment function.

```
Hostname(config-wids)# no countermeasures fuzzy-enable
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Platform** N/A

**Description**

### 1.15 countermeasures fuzzy-keyword

Use this command to configure a fuzzy containment keyword.

Use the **no** form of this command to remove the fuzzy containment keyword.

**countermeasures fuzzy-keyword** *string*

**no countermeasures fuzzy-keyword** *string*

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>string</i>	Indicates the fuzzy containment keyword, which is case-insensitive and stored in lowercase.

**Defaults** By default, no fuzzy containment is configured.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** The configuration takes effect only after the **countermeasures fuzzy-enable** command is executed. When the

containment mode covers the SSID mode, rogue APs whose SSIDs contain the configured keyword will be contained. The fuzzy containment keyword takes effect only in SSID mode. The keyword is case-insensitive. For example, assume that the configured fuzzy containment keyword is test. There are 2<sup>4</sup> uppercase and lowercase combinations of test. Once the fuzzy containment keyword is set to any of the combinations, APs whose SSIDs contain any combination of ruijie can be identified.

**Configuration** The following example configures a fuzzy containment keyword.

**Examples**

```
Hostname(config)# wids
Hostname(config-wids)# countermeasures fuzzy-keyword test
```

The following example removes the fuzzy containment keyword.

```
Hostname(config)# wids
Hostname(config-wids)# no countermeasures fuzzy-keyword test
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A  
**Description**

### 1.16 device aging duration

Use this command to configure device aging duration. Use the **no** form of this command to restore the default setting.

- device aging duration *time***
- no device aging duration**

**Parameter Description**

Parameter	Description
<i>time</i>	Indicates device aging duration in the range from 500 to 5000 in the unit of seconds.

**Defaults** The default is 1200 seconds.

**Command Mode** WIDS configuration mode

**Usage Guide** Use this command to configure device aging duration.

**Configuration** The following example sets the device aging duration to 1000 seconds.

**Examples**

```
Hostname(config-wids)# device aging duration 1000
```

The following example restores the device aging duration to the default setting.

```
Hostname(config-wids)# no device aging duration
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show running-config** command to show the configuration.

**Platform** N/A  
**Description**

### 1.17 device attack mac-address

Use this command to configure an entry for static attack list. Use the **no** form of this command to delete a configured entry of the static attack list.

**device attack mac-address H.H.H**  
**no device attack mac-address H.H.H**

Parameter Description	Parameter	Description
	H.H.H	Indicates the device with this source MAC address is subjected to the countermeasures.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** This configuration is one of the policies for detecting rogue devices.

**Configuration Examples** The following example configures the device with the static attack source MAC address of 0000.0000.0001.

```
Hostname(config-wids)# device attack mac-address 0000.0000.0001
```

The following example deletes the static attack list with its source MAC address of 0000.0000.0001.

```
Hostname(config-wids) #no device attack mac-address 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Notifications** When the MAC address is already in the permissible MAC address list, the following notification will be displayed:  
 The mac address has been permitted!

**Platform** N/A  
**Description**

### 1.18 device attack max

Use this command to configure the maximum number of the static attack list.  
 Use the **no** form of this command to restore the default setting.

**device attack max** *num*  
**no device attack max**

Parameter Description	Parameter	Description
	<i>num</i>	Specifies the maximum number of the static attack list in the range from 1 to 1024.

**Defaults** The default is 512.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of the static attack list to 900.

**Examples**

```
Hostname(config-wids)# device attack max 900
```

The following example restores the default setting.

```
Hostname(config-wids)# no device attack max
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.19 device black-ssid

Use this command to configure an entry for the SSID blacklist. Use the **no** form of this command to remove an entry from the SSID blacklist.

**device black-ssid** *ssid*  
**no device black-ssid** *ssid*

Parameter Description	Parameter	Description
	<i>ssid</i>	The SSID configured to the blacklist. The detection device detects this SSID for countermeasures in WIDS config mode,
<b>Defaults</b>	N/A	
<b>Command Mode</b>	WIDS configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	<p>The following example configures SSID: my-vlan to the SSID blacklist.</p> <pre>Hostname (config-wids) # device black-ssid my-wlan</pre> <p>The following example removes SSID: my-vlan from the SSID blacklist.</p> <pre>Hostname (config-wids) # no device black-ssid my-wlan</pre>	
<b>Platform Description</b>	N/A	

## 1.20 device detected-ap-max

Use this command to configure the maximum number of detected AP list members. Use the **no** form of this command to restore the default setting.

**device detected-ap-max num**  
**no device detected-ap-max num**

Parameter Description	Parameter	Description
	<b>detected-ap-max num</b>	The maximum number of detected AP list members.
<b>Defaults</b>	The default is 2048.	
<b>Command Mode</b>	WIDS configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	<p>The following example configures the maximum number of detected AP list members to 1000.</p> <pre>Hostname#configure Hostname (config) #wids Hostname (config-wids) # device detected-ap-max 1000</pre>	



**Platform**  
**Description** N/A

### 1.21 device friendly-flags

Use this command to configure the friendly flag on a device. Use the **no** form of this command to restore the default setting.

**device friendly-flags** *value*

**no device friendly-flags**

Parameter	Parameter	Description
<b>Description</b>	<i>value</i>	Friendly flag value in the range from 1 to 4294967295.

**Defaults** The default is 0.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** By configuring the friendly flag, AP is able to recognize a friendly AP. The default is random configuration.

**Configuration** The following example configures the friendly flag to 4294967295.

```
Hostname(config-wids)# device friendly-flags 4294967295
```

The following example restores the friendly flag to the default setting.

```
Hostname(config-wids)# no device friendly-flags
```

**Platform**  
**Description** N/A

### 1.22 device max-black-ssid

Use this command to configure the maximum number of the SSID blacklist. Use the **no** form of this command to restore the default setting.

**device max-black-ssid** *num*

**no device max-black-ssid**

Parameter	Parameter	Description
<b>Description</b>	<i>num</i>	The maximum number of the SSID blacklist in the range from 1 to 1024.

**Defaults** The default is 512.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the maximum number of the SSID blacklist to 900.

```
Hostname(config-wids)# device max-black-ssid 900
```

The following example restores the default setting.

```
Hostname(config-wids)# no device max-black-ssid
```

**Platform** N/A  
**Description**

### 1.23 device mode

Use this command to configure the working mode of the AP. Use the **no** form of this command to restore the default setting.

```
device mode { hybrid | monitor [ radio ] }
```

```
no countermeasures mode
```

Parameter	Parameter	Description
Description	<b>monitor</b>	Indicates AP works in the monitor mode.
	<b>normal</b>	Indicates AP works in the normal mode.
	<b>hybrid</b>	Indicates AP works in the hybrid mode.

**Defaults** The AP works in the normal mode by default.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the working mode of the AP to **hybrid**.

```
Hostname#configure
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# wids
Hostname(config-wids)#device mode hybrid
```

The following example sets the working mode of the radio 3 to **monitor**.

```
Hostname#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# wids
```

```
Hostname(config-wids)#device mode monitor
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.24 device permit mac-address

Use this command to configure an entry for the permissible MAC address list. Use the **no** form of this command to delete an entry from the permissible MAC address list.

**device permit mac-address** *H.H.H*  
**no device permit mac-address** *H.H.H*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** This configuration is one of the policies for detecting rogue devices.

**Configuration Examples** The following example configures the device with the permissible source MAC address of 0000.0000.0001.

```
Hostname(config-wids)# device permit mac-address 0000.0000.0001
```

The following example deletes the device with the permissible source MAC address of 0000.0000.0001.

```
Hostname(config-wids)# no device permit mac-address 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids permitted mac-address** command to view the configured entry in the permissible MAC address list.

**Notifications** When the MAC address is already in the attack list, the following notification will be displayed:  
 The mac address has been attacked!

**Common Errors** N/A

**Platform** N/A  
**Description**

### 1.25 device permit mac-address max

Use this command to configure the maximum entry number of the permissible MAC address list.  
 Use the **no** form of this command to restore the default setting.

**device permit mac-address max** *num*  
**no device permit mac-address max**

Parameter Description	Parameter	Description
	<i>num</i>	Specifies the maximum entry number of the permissible MAC address list in the range from 1 to 2048.

**Defaults** The default is 1024.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the maximum entry number of the permissible MAC address list to 1000.

```
Hostname(config-wids)# device permit mac-address max 1000
```

The following example restores the default setting.

```
Hostname(config-wids)# no device permit mac-address max
```

Related Commands	Command	Description
	N/A	N/A

**Verification** N/A  
 Run the **show running-config** command to view the configured maximum entry number of the permissible MAC address list.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.26 device permit ssid

Use this command to configure an entry for the permissible SSID list. Use the **no** form of this command to delete an entry for the permissible SSID list.

**device permit ssid** *ssid*

**no device permit ssid** *ssid*

Parameter	Parameter	Description
Description	<i>ssid</i>	Configures this SSID to the permissible SSID list.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** This configuration is one of the policies for detecting rogue devices.

**Configuration Examples** The following example configures SSID: my-wlan to the permissible SSID list.

```
Hostname(config-wids)# device permit ssid my-wlan
```

The following example removes SSID: my-wlan from the permissible SSID list.

```
Hostname(config-wids)# no device permit ssid my-wlan
```

**Verification** Run the **show wids permitted ssid** to view SSIDs in the permissible SSID list.

**Notifications** When the length of the SSID to be configured exceeds 32 characters, the following notification will be displayed:  
SSID not more than 32 characters!

**Common Errors** N/A

**Platform Description** N/A

## 1.27 device permit max-ssid

Use this command to configure the maximum number of the permissible SSID list members. Use the **no** form of this command to restore the default setting.

**device permit max-ssid** *num*

**no device permit max-ssid**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>		
	<i>num</i>	Specifies the maximum number of permissible SSID list members in the range from 1 to 1024.

**Defaults** The default is 512.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of the permissible SSID list members to 900.

**Examples**

```
Hostname(config-wids)# device permit max-ssid 900
```

The following example restores the default setting.

```
Hostname(config-wids)# no device permit max-ssid
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	N/A	N/A

**Verification** Run the **show running-config** command to view the configured maximum number of the permissible SSID list members.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.28 device permit vendor bssid

Use this command to configure an entry for the permissible vendor list. Use the **no** form of this command to delete an entry for the permissible vendor list.

**device permit vendor bssid H.H.H**

**no device permit vendor bssid H.H.H**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<i>H.H.H</i>	Indicates this vendor’s address is a permissible address.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** The vendor number is used to configure the first three bytes of a MAC address. Do not configure multiple MAC addresses with the same vendor number. This configuration is one of the policies for detecting rogue devices.

**Configuration** The following example configures the MAC address 0000.0000.0001 into the permissible vendor list.

**Examples**

```
Hostname(config-wids)# device permit vendor bssid 0000.0000.0001
```

The following example deletes the MAC address 0000.0000.0001 from the permissible vendor list.

```
Hostname(config-wids)#no device permit vendor bssid 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids permitted vendor** command to view the configured entry in the permissible vendor list.

**Notifications** When a vendor is already in the permissible vendor list, the following notification will be displayed:  
The permitted vendor[*vendor-mac*] already exists!

**Common Errors** N/A

**Platform Description** N/A

### 1.29 device permit vendor bssid max

Use this command to configure the maximum number of the permissible vendor list members.

Use the **no** form of this command to restore the default setting.

**device permit vendor bssid max** *num*

**no device permit vendor bssid max**

Parameter Description	Parameter	Description
	<i>num</i>	

**Defaults** The default is 512.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of the permissible vendor list members to 1000.

**Examples**

```
Hostname(config-wids)# device permit vendor bssid max 1000
```

The following example restores the default setting.

```
Hostname(config-wids)#no device permit vendor bssid max
```

**Related**  
**Commands**

Command	Description
N/A	N/A

**Verification** Run the **show running-config** command to view the configured maximum number of the permissible vendor list members.

**Notifications** N/A

**Common Errors** N/A

**Platform**  
**Description** N/A

### 1.30 device unknown-sta dynamic-enable

Use this command to enable dynamic unknown STA detection. Use the **no** form of this command to restore the default setting.

**device unknown-sta dynamic-enable**

**no device unknown-sta dynamic-enable**

**Parameter**  
**Description**

Parameter	Description
N/A	N/A

**Defaults** The function is disabled by default.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** This command takes effect only when the AP works in the normal mode.



<b>Configuration</b>	The following example enables dynamic unknown STA detection.
<b>Examples</b>	<pre>Hostname(config-wids)# device unknown-sta dynamic-enable</pre>
	The following example disables dynamic unknown STA detection.
	<pre>Hostname(config-wids)# no device unknown-sta dynamic-enable</pre>
<b>Verification</b>	Run the <b>show running-config</b> command to view the enabling status of dynamic unknown STA detection.
<b>Notifications</b>	N/A
<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

### 1.31 device unknown-sta mac-address

Use this command to configure an entry for the static unknown STA list. Use the **no** form of this command to delete an entry for the static unknown STA list.

**device unknown-sta mac-address** *H.H.H*

**no device unknown-sta mac-address** *H.H.H*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	Indicates that the user of this MAC address is unknown STA.

<b>Defaults</b>	N/A
<b>Command Mode</b>	WIDS configuration mode
<b>Usage Guide</b>	This command is one of the policies for detecting rogue devices.
<b>Configuration Examples</b>	The following example configures the MAC address 0000.0000.0001 to the unknown STA list.
	<pre>Hostname(config-wids)# device unknown-sta mac-address 0000.0000.0001</pre>
	The following example removes the MAC address 0000.0000.0001 from the unknown STA list.
	<pre>Hostname(config-wids)# no device unknown-sta mac-address 0000.0000.0001</pre>
<b>Verification</b>	Run the <b>show wids unknown-sta</b> command to view the configured entry in the static unknown STA list.

Notifications	N/A
Common Errors	N/A
Platform Description	N/A

## 1.32 device unknown-sta mac-address max

Use this command to configure the maximum number of the unknown STA list members. Use the **no** form of this command to restore the default setting,

**device unknown-sta mac-address max** *num*

**no device unknown-sta mac-address max**

Parameter Description	Parameter	Description
	<i>num</i>	The maximum number of the unknown STA list members in the range from 1 to 256.

**Defaults** The default is 128.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the maximum number of the unknown STA list members to 200.

```
Hostname(config-wids)# device unknown-sta mac-address max 200
```

The following example restores the maximum number of the unknown STA list members to the default setting.

```
Hostname(config-wids)# no device unknown-sta mac-address max
```

**Verification** Run the **show running-config** command to view the configured maximum number of the unknown STA list members.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.33 dynamic-blacklist enable

Use this command to enable the dynamic blacklist. Use the **no** form of this command to restore the default setting.

**dynamic-blacklist enable**

**no dynamic-blacklist enable**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the dynamic blacklist.

```
Hostname(config-wids)# dynamic-blacklist enable
```

The following example disables the dynamic blacklist.

```
Hostname(config-wids)#no dynamic-blacklist enable
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show running-config** command to view the enabling status of the dynamic blacklist function.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.34 dynamic-blacklist lifetime

Use this command to configure the dynamic blacklist entry lifetime. Use the **no** form of this command to restore the default setting.

**dynamic-blacklist lifetime** *time*

**no dynamic-blacklist lifetime**

Parameter Description	Parameter	Description
	<i>time</i>	Indicates the dynamic blacklist entry lifetime in the range from 60 to 86400 in the unit of seconds.

**Defaults** The default is 300 seconds.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the dynamic blacklist entry lifetime to 600 seconds.

```
Hostname(config-wids)# dynamic-blacklist lifetime 600
```

The following example restores the default setting.

```
Hostname(config-wids)# no dynamic-blacklist lifetime
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show running-config** command to view the dynamic blacklist entry lifetime.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.35 dynamic-blacklist ap-max

Use this command to configure the maximum number of dynamic blacklist members on the AP. Use the **no** form of this command to restore the default setting.

**dynamic-blacklist ap-max num**

**no dynamic-blacklist ap-max**

Parameter Description	Parameter	Description
	<i>num</i>	The maximum number of dynamic blacklist members on the AP in the range from 1 to 4096.

<b>Defaults</b>	The default is 2048.
<b>Command</b>	WIDS configuration mode
<b>Mode</b>	
<b>Usage Guide</b>	N/A
<b>Configuration</b>	The following example configures the maximum number of dynamic blacklist members on the AP to 1000.
<b>Examples</b>	<pre>Hostname (config-wids) # dynamic-blacklist ap-max 1000</pre>
	The following example restores the default setting.
	<pre>Hostname (config-wids) #no dynamic-blacklist ap-max</pre>
<b>Verification</b>	Run the <b>show running-config</b> command to view the configured maximum number of dynamic blacklist members on the AP.
<b>Platform</b>	N/A
<b>Description</b>	

### 1.36 hybrid-scan radio

Use this command to enable the radio scan. Use the **disable** form of this command to disable the radio scan.

**hybrid-scan radio num enable**

**hybrid-scan radio num disable**

Parameter Description	Parameter	Description
	<b>radio num</b>	Radio number.

<b>Defaults</b>	This function is enabled by default.
<b>Command</b>	WIDS configuration mode
<b>Mode</b>	
<b>Usage Guide</b>	N/A
<b>Configuration</b>	The following example disables the scan for radio 1.
<b>Examples</b>	<pre>Hostname#configure Hostname (config) # wids Hostname (config-wids) # hybrid-scan radio 1 disable</pre>

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.37 kickout client

Use this command to kick out associate users.

**kickout client** *H.H.H*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	The MAC address of the user to kick out.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** Use this command to disconnect a specified STA association.

**Configuration Examples** The following example kicks out the MAC address 0000.0000.0001.

```
Hostname(config-wids)# kickout client 0000.0000.0001
```

**Platform Description** N/A

## 1.38 kickout threshold

Use this command to kick out the low-rate STA. Use the **no** form of this command to restore the default setting.

**kickout threshold** *rate*

**no kickout threshold**

Parameter Description	Parameter	Description
	<i>rate</i>	Packet sending-receiving rate in the range from 0 to 130 in the unit of Mbps.

**Defaults** The default is 0, indicating not filtering low-rate STA.

**Command Mode** WIDS configuration mode

**Usage Guide** This command is used to filter the low-rate STA. When the wireless access end detects that the sending-receiving rate of STA is less than the configured threshold, it disconnects the association.

**Configuration** The following example disables the filtering.

**Examples** `Hostname(config-wids)# no kickout threshold`

Related Commands	Command	Description
	<code>wids</code>	

**Verification** Run the **show running-config** command to view the threshold for filtering out low-rate STAs.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.39 reset attack-list all

Use this command to clear the entries of all attack lists.

**reset attack-list all**

Parameter Description	Parameter	Description
	N/A	

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example clears the entries of all attack lists.

**Examples** `Hostname(config-wids)# reset attack-list all`

Related	Command	Description
---------	---------	-------------

<b>Commands</b>		
	N/A	N/A

**Verification** Run the **show wids attacklist** command to check whether the entries of all attack lists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.40 reset black-ssid all

Use this command to clear the entries of the SSID blacklist.

**reset black-ssid all**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the entries of the SSID blacklist.

```
Hostname(config-wids)# reset black-ssid all
```

**Verification** Run the **show wids black-ssid** command to check whether the entries of the SSID blacklist are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A



## 1.41 reset detected

Use this command to reset the device list detected in a WLAN.

**reset detected** { **all** | **adhoc** | **rogue** { **ap** | **client** } | **mac-address** *H.H.H* }

Parameter	Parameter	Description
Description	<b>all</b>	Indicates you reset all devices detected in a WLAN.
	<b>adhoc</b>	Indicates you reset the detected adhoc client.
	<b>rogue ap</b>	Indicates you reset the detected Rogue AP.
	<b>rogue client</b>	Indicates you reset the detected Rogue client.
	<b>mac-address</b> <i>H.H.H</i>	Indicates you reset the device with the source MAC address H.H.H.

**Defaults** N/A

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example resets the rogue APs detected in a WLAN.

**Examples**

```
Hostname(config-wids)# reset detected rogue ap
```

The following example resets the information of detected rogue APs.

```
Hostname(config-wids)# reset detected rogue ap
```

The following example resets the information of detected device with MAC address 0000.0000.0001.

```
Hostname(config-wids)# reset detected mac-address 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids detected** command to check whether information about devices detected in a WLAN in the device list is cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.42 reset dynamic-blacklist

Use this command to reset dynamic blacklist entries.

**reset dynamic-blacklist** { **all** | **mac-address** *H.H.H* }

Parameter	Parameter	Description
Description	<b>all</b>	Indicates you reset all dynamic blacklist entries.
	<b>mac-address</b> <i>H.H.H</i>	Indicates you reset the dynamic blacklist entry with the source MAC address H.H.H.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example resets the dynamic blacklist entry with the source MAC address 0000.0000.0001.

```
Hostname(config-wids)# reset dynamic-blacklist mac-address 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids blacklist dynamic** command to check whether the dynamic blacklist entry is cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.43 reset fuzzy-keyword all

Use this command to clear the fuzzy containment keywords.

**reset fuzzy-keyword all**

Parameter	Parameter	Description
Description		

N/A	N/A
-----	-----

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the fuzzy containment keywords.

```

Hostname (config) # wids
Hostname (config-wids) # reset fuzzy-keyword all
    
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids fuzzy-keyword** command to check whether the fuzzy containment keywords are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.44 reset permit-mac all

Use this command to clear the entries of all permissible MAC address lists.

**reset permit-mac all**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example clears the entries of all permissible MAC address lists.

**Examples**

```
Hostname(config-wids)# reset permit-mac all
```

**Related Commands**

Command	Description
N/A	N/A

**Verification** Run the **show wids permitted mac-address** command to check whether the entries of all permissible MAC address lists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.45 reset permit-ssid all

Use this command to clear the entries of all permissible SSID lists.

**reset permit-ssid all**

**Parameter Description**

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example clears the entries of all permissible SSID lists.

**Examples**

```
Hostname(config-wids)# reset permit-ssid all
```

**Related Commands**

Command	Description
N/A	N/A

**Verification** Run the **show wids permitted ssid** command to check whether the entries of all permissible SSID lists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.46 reset permit-vendor all

Use this command to clear the entries of all permissible vendor lists.

**reset permit-vendor all**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the entries of all permissible vendor lists.

```
Hostname(config-wids)# reset permit-vendor all
```

Related Commands	Command	Description
		N/A

**Verification** Run the **show wids permitted vendor** command to check whether the entries of all permissible vendor lists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.47 reset rogue-ap detected

Use this command to clear the information from rogue AP detection according to *CMCC WLAN AC-AP Interoperability Specification*.

**reset rogue-ap detected**

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	WIDS configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example clears the information from rogue AP detection: <pre>Hostname(config-wids)#reset rogue-ap detected</pre>	
Verification	Run the <b>show wids rogue-ap detected</b> command to check whether the information from rogue AP detection is cleared.	
Notifications	N/A	
Common Errors	N/A	
Platform Description	N/A	

### 1.48 reset ssid-filter

Use this command to remove all SSIDs or a specified SSID from blacklists and whitelists.

**reset ssid-filter { ssid all | in-ssid ssid }**

Parameter Description	Parameter	Description
	<b>ssid all</b>	All SSIDs.
	<b>in-ssid ssid</b>	The specified SSID

<b>Defaults</b>	N/A
<b>Command Mode</b>	WIDS configuration mode
<b>Default Level</b>	14
<b>Usage Guide</b>	N/A
<b>Configuration</b>	The following example removes all SSIDs from blacklists and whitelists.
<b>Examples</b>	<pre>Hostname(config-wids)#reset ssid-filter ssid all</pre>
<b>Verification</b>	Run the <b>show wids ssid-filter</b> command to check whether all SSIDs or a specified SSID is removed from blacklists and whitelists.
<b>Notifications</b>	When a specified SSID does not exist, the following notification will be displayed: <pre>There is no SSID[ssid] to filter!</pre>
<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

## 1.49 reset ssid-filter blacklist all

Use this command to remove all SSIDs from blacklists.

**reset ssid-filter blacklist all**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example clears all the SSIDs from blacklists,

**Examples**

```
Hostname(config-wids)# reset ssid-filter blacklist all
```

<b>Verification</b>	Run the <b>show wids ssid-filter blacklist all</b> command to check whether all SSIDs are removed from blacklists.
<b>Notifications</b>	N/A
<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

## 1.50 reset ssid-filter blacklist all in-ssid

Use this command to remove a specified SSID from blacklists.

**reset ssid-filter blacklist all in-ssid *string***

Parameter Description	Parameter	Description
	<i>string</i>	Removes specified SSIDs from the blacklist.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example removes SSID: my-vlan from blacklists.

**Examples** `Hostname(config-wids)# reset ssid-filter blacklist all in-ssid my-wlan`

**Verification** Run the **show wids ssid-filter blacklist all in-ssid *string*** command to check whether the specified SSID is removed from blacklists.

**Notifications** When a specified SSID does not exist, the following notification will be displayed:  
There is no SSID[*ssid*] to filter!

**Common Errors** N/A

**Platform Description** N/A

## 1.51 reset ssid-filter whitelist all

Use this command to remove all SSIDs from whitelists.



**reset ssid-filter whitelist all**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A
<b>Defaults</b>	N/A	
<b>Command Mode</b>	WIDS configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example removes all SSIDs from whitelists.	
	<pre>Hostname(config-wids)# reset ssid-filter whitelist all</pre>	
<b>Verification</b>	Run the <b>show wids ssid-filter whitelist all</b> command to check whether all SSIDs are removed from whitelists.	
<b>Notifications</b>	N/A	
<b>Common Errors</b>	N/A	
<b>Platform Description</b>	N/A	

### 1.52 reset ssid-filter whitelist all in-ssid

Use this command to remove a specified SSID from whitelists.

**reset ssid-filter whitelist all in-ssid *string***

<b>Parameter Description</b>	Parameter	Description
	<i>string</i>	Removes all the whitelists from a specified SSID.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	WIDS configuration mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example removes SSID: my-wlan from whitelists.	
	<pre>Hostname(config-wids)# reset ssid-filter whitelist all in-ssid my-wlan</pre>	

**Verification** Run the **show wids ssid-filter whitelist all in-ssid** *string* command to check whether the specified SSID is removed from whitelists.

**Notifications** When a specified SSID does not exist, the following notification will be displayed:  
There is no SSID[*ssid*] to filter!

**Common Errors** N/A

**Platform Description** N/A

### 1.53 reset static-blacklist all

Use this command to clear the entries of all static blacklists.

**reset static-blacklist all**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the entries of all static blacklists.

```
Hostname(config-wids)# reset static-blacklist all
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids blacklist static** command to check whether the entries of all static blacklists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.54 reset statistic all

Use this command to clear attack detection statistics.

**reset statistic all**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	WIDS configuration mode	
Usage Guide	N/A	
Configuration	The following example clears attack detection statistics.	
Examples	<pre>Hostname(config-wids)# reset statistic all</pre>	
Platform Description	N/A	

## 1.55 reset unknown-sta all

Use this command to clear the entries of unknown STA lists.

**reset unknown-sta all**

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	WIDS configuration mode	
Usage Guide	N/A	
Configuration	The following example clears the entries of unknown STA lists.	
Examples	<pre>Hostname(config-wids)# reset unknown-sta all</pre>	
Verification	Run the <b>show wids unknown-sta</b> command to check whether the entries of unknown STA lists are cleared.	

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.56 reset user-isolation-permit-list all

Use this command to clear the entries of all permissible lists for user isolation.

**reset user-isolation-permit-list all**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example clears the entries of all permissible lists for user isolation.

```
Hostname(config-wids)# reset user-isolation-permit-list all
```

Related Commands	Command	Description
		N/A

**Verification** Run the **show wids user-isolation permit-mac** command to check whether the entries of all permissible lists for user isolation are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.57 reset whitelist all

Use this command to clear the entries of all whitelists.

**reset whitelist all**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example clears the entries of all whitelists.

```
Hostname(config-wids)# reset whitelist all
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids whitelist** command to check whether the entries of all whitelists are cleared.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.58 scan-channels channels

Use this command to configure the scan channel. Use the **no** form of this command to restore the default setting.

**scan-channels { 802.11a | 802.11b } channels *num1 num2...num13***

**no scan-channels { 802.11a | 802.11b }**

Parameter	Parameter	Description
Description	<b>802.11a</b>	5 GHz channel. By default, no scan channel is configured.

<b>802.11b</b>	2.4 GHz channel. By default, no scan channel is configured.
<b>channels num</b>	Channel value.

**Defaults** No scan channel is configured by default.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the 5GHz scan channel as 149 153 157.

```

Examples
Hostname#configure
Hostname(config)# wids
Hostname(config-wids)# scan-channels 802.11a channels 149 153 157
    
```

**Platform** N/A  
**Description**

### 1.59 scan-channels dual-band

Use this command to configure automatic channel scanning between two frequency bands.

**scan-channels dual-band radio radio-id**

Use the no form of this command to restore the default setting.

**no scan-channels dual-band radio radio-id**

Parameter Description	Parameter	Description
	<i>radio-id</i>	Indicates the radio ID.

**Defaults** By default, this function is disabled.

**Command** WIDS configuration mode

**Mode**

**Default Level** 14

**Usage Guide** The RF modules of partial APs support both the 2.4 GHz and 5 GHz frequency bands. When the RF modules are used for channel scanning, this command can be used for automatic channel scanning between the two frequency bands, to obtain the scanning results of these two frequency bands and perform containment. After the frequency bands are switched, channels configured by running the **scan-channels { 802.11a | 802.11b } channels** command are scanned. In addition, for some APs that have channel restrictions, the restricted channels will be automatically skipped during channel scanning.

**Configuration** The following example enables dual-band scanning on the Radio3 of AP1.

```

Examples
Hostname# configure terminal
Hostname(config)# wids
Hostname(config-wids)# scan-channels dual-band radio 3
    
```

**Verification** Run the **show running-config** command to show the configuration.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.60 show wids attack-list

Use this command to display the WIDS static attack list.

**show wids attack-list**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays the WIDS static attack list.

```

Examples
Hostname# show wids attack-list
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.61 show wids blacklist

Use this command to display the static or dynamic blacklist.

**show wids blacklist { static | dynamic }**

Parameter	Parameter	Description
Description	<b>static</b>	Displays the static blacklist.
	<b>dynamic</b>	Displays the dynamic blacklist.

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the static blacklist.

```
Hostname# show wids blacklist static
```

The following example displays the dynamic blacklist.

```
Hostname# show wids blacklist dynamic
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.62 show wids black-ssid

Use this command to display the SSID blacklist.

**show wids black-ssid**

Parameter	Parameter	Description
Description	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A



**Configuration** The following example displays the SSID blacklist.

**Examples** `Hostname# show wids black-ssid`

**Platform** N/A  
**Description**

### 1.63 show wids detected

Use this command to display the devices detected in a WLAN.

**show wids detected** { **adhoc** | **all** | **friendly ap** | **fuzzy-ssid ssid** | **interfering ap** | **mac-address H.H.H** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } }

Parameter Description	Parameter	Description
	<b>adhoc</b>	Displays the detected ad-hoc network.
	<b>all</b>	Displays all devices detected in a WLAN.
	<b>friendly ap</b>	Displays the detected friendly AP.
	<b>interfering ap</b>	Displays the detected interference AP.
	<b>rogue adhoc-ap</b>	Displays the detected Rogue ad-hoc AP.
	<b>rogue ap</b>	Displays the detected Rogue AP.
	<b>rogue client</b>	Displays the detected Rogue Client.
	<b>rogue config-ap</b>	Displays the detected Rogue config AP.
	<b>rogue ssid -ap</b>	Displays the detected Rogue SSID AP.
	<b>mac-address H.H.H</b>	Displays the detected device with the source MAC address H.H.H.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the Rogue AP detected in a WLAN.

**Examples** `Hostname# show wids detected rogue ap`

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.64 show wids fuzzy-keyword

Use this command to display the fuzzy containment keyword.

**show wids fuzzy-keyword**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	N/A	N/A
<b>Command Mode</b>	Privileged EXEC mode	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example displays the fuzzy containment keyword.	
	<pre>Hostname# show wids fuzzy-keyword</pre>	
<b>Platform Description</b>	N/A	

## 1.65 show wids ssid-filter

Use this command to display the blacklists and whitelists for all SSIDs or a specified SSID.

**show wids ssid-filter { blacklist { all | in-ssid *string* } | ssid all | whitelist { all | in-ssid *string* } }**

<b>Parameter Description</b>	<b>Parameter</b>	<b>Description</b>
	<b>blacklist all</b>	Displays the blacklists for all SSIDs.
	<b>blacklist in-ssid <i>string</i></b>	Displays the blacklists for a specified SSID.
	<b>ssid all</b>	Displays the blacklists and whitelists for all SSIDs.
	<b>white all</b>	Displays the whitelists for all SSIDs.
	<b>whitelist in-ssid <i>string</i></b>	Displays the whitelists for a specified SSID.
<b>Defaults</b>	N/A	
<b>Command Mode</b>	Privileged EXEC mode.	
<b>Usage Guide</b>	N/A	
<b>Configuration Examples</b>	The following example displays the blacklists for all SSIDs.	
	<pre>Hostname# show wids ssid-filter blacklist all</pre>	

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

### 1.66 show wids permitted

Use this command to display the MAC address, SSID, and vendor lists trusted in a WLAN.

**show wids permitted { mac-address | ssid | vendor }**

Parameter Description	Parameter	Description
	<b>mac-address</b>	
<b>ssid</b>		Displays the trusted SSID list.
<b>vendor</b>		Displays the trusted vendor list.

Defaults N/A

Command Privileged EXEC mode  
Mode

Usage Guide N/A

Configuration The following example displays the SSID list trusted in WLAN.

Examples 

```
Hostname# show wids permitted ssid
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A  
Description

### 1.67 show wids statistics

Use this command to display the IDS attack detection statistics.

**show wids statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following example displays the IDS attack detection statistics.

**Examples** `Hostname# show wids statistics`

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

### 1.68 show wids unknown-sta

Use this command to display the entries of unknown STA lists.

**show wids unknown-sta**

Parameter Description	Parameter	Description
	N/A	N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the entries of unknown STA lists.

**Examples** `Hostname# show wids unknown-sta`

**Platform Description** N/A

### 1.69 show wids user-isolation permit-mac

Use this command to display the information of the permissible MAC address list for user isolation.

**show wids user-isolation permit-mac**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	<p>The following example displays the information of the permissible MAC address list for user isolation.</p> <pre>Hostname# show wids user-isolation permit-mac</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
<b>Platform Description</b>	N/A				

### 1.70 show wids whitelist

Use this command to display the whitelist.

**show wids whitelist**

<b>Parameter Description</b>	<table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
<b>Defaults</b>	N/A				
<b>Command Mode</b>	Privileged EXEC mode				
<b>Usage Guide</b>	N/A				
<b>Configuration Examples</b>	<p>The following example displays the whitelist.</p> <pre>Hostname# show wids whitelist</pre>				
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				

**Platform** N/A  
**Description**

## 1.71 ssid-filter max

Use this command to configure the maximum number of the blacklist and whitelist members for SSIDs. Use the **no** form of this command to restore the default setting.

**ssid-filter max** *num*

**no ssid-filter max**

Parameter	Parameter	Description
Description	<i>num</i>	The maximum number of the blacklist and whitelist members in the range from 1 to 128.

**Defaults** The default is 64.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the maximum number of the blacklist and whitelist members for SSIDs as 40.  
**Examples**

```
Hostname(config-wids)# ssid-filter max 40
```

The following example restores the default setting.

```
Hostname(config-wids)#no ssid-filter max
```

**Platform** N/A  
**Description**

## 1.72 ssid-filter blacklist mac-address in-ssid

Use this command to configure an entry for a specified SSID blacklist. Use the **no** form of this command to restore the default setting.

**ssid-filter blacklist mac-address** *H.H.H* [ **name** *another-name* ] **in-ssid** *string*

**no ssid-filter blacklist mac-address** *H.H.H* **in-ssid** *string*

Parameter	Parameter	Description
Description	<i>H.H.H</i>	The MAC address of an entry to configure.

<i>string</i>	SSID.
<i>another-name</i>	The another-name of the MAC address in the specified SSID blacklist.

**Defaults** N/A

**Command** WIDS configuration mode

**Mode**

**Usage Guide** This command is not allowed to use when there is the same entry in the SSID whitelist. One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name. The another-name is null if it is not configured.

**Configuration** The following example configures MAC 0000.0000.0001 for the blacklist of SSID: my-wlan.

**Examples**

```
Hostname(config-wids)# ssid-filter blacklist mac-address 0000.0000.0001
in-ssid my-wlan
```

The following example restores the default setting.

```
Hostname(config-wids)# no ssid-filter blacklist mac-address 0000.0000.0001
in-ssid my-wlan
```

**Platform** N/A  
**Description**

### 1.73 ssid-filter blacklist max

Use this command to set the maximum number of the SSID blacklist members. Use the **no** form of this command to restore the default setting.

**ssid-filter blacklist max num**

**no ssid-filter blacklist max**

Parameter	Parameter	Description
Description	<i>num</i>	The maximum number of the SSID blacklist members in the range from 1 to 2,048.

**Defaults** The default is 256.

**Command** WIDS configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of the blacklist members as 50.

**Examples**

```
Hostname(config-wids)# ssid-filter blacklist max 50
```

The following example restores the default setting.

```
Hostname(config-wids)# no sid-filter blacklist max
```

**Verification** Run the **show running-config** command to show the configuration.

**Notifications** N/A

**Common Errors** N/A

**Platform** N/A

**Description**

### 1.74 ssid-filter whitelist mac-address in-ssid

Use this command to configure an entry for a specified SSID whitelist. Use the **no** form of this command to restore the default setting.

**ssid-filter whitelist mac-address *H.H.H* [ name *another-name* ] in-ssid *string***

**no ssid-filter whitelist mac-address *H.H.H* in-ssid *string***

Parameter Description	Parameter	Description
	<i>H.H.H</i>	The MAC address of the entry configured for the specified SSID whitelist.
	<i>string</i>	The specified SSID.
	<i>another-name</i>	The another-name of the MAC address in the specified SSID whitelist.

**Defaults** N/A

**Command** WIDS configuration mode

**Mode**

**Usage Guide** This command is not allowed to use when there is the same entry in the SSID blacklist. One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name. The another-name is null if it is not configured.

**Configuration** The following example configures MAC 0000.0000.0001 to the whitelist of SSID: my-wlan.

**Examples**

```
Hostname(config-wids)# ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

The following example restores the default setting.

```
Hostname(config-wids)# no ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

**Platform** N/A



Description

### 1.75 ssid-filter whitelist max

Use this command to set the maximum number of the SSID whitelist members. Use the **no** form of this command to restore the default setting.

**ssid-filter whitelist max** *num*  
**no ssid-filter whitelist max**

Parameter	Parameter	Description
Description	<i>num</i>	The maximum number of the SSID whitelist members in the range from 1 to 2,048.

**Defaults** The default is 256

**Command Mode** WIDS configuration mode

**Usage Guide** N/

**Configuration Examples** The following example sets the maximum number of the whitelist members as 50.

```
Hostname(config-wids)# ssid-filter whitelist max 50
```

The following example restores the default setting.

```
Hostname(config-wids)# no sid-filter whitelist max
```

**Platform Description** N/A

### 1.76 static-blacklist mac-address

Use this command to configure an entry for the static blacklist. Use the **no** form of this command to delete the static blacklist

**static-blacklist mac-address** *H.H.H* [ **name** *another-name* ]  
**no static-blacklist mac-address** *H.H.H*

Parameter	Parameter	Description
Description	<i>H.H.H</i>	Indicates you set the device with the source MAC address H.H.H as a static blacklist entry.
	<b>no</b>	Indicates you delete the static blacklist.
	<i>another-name</i>	The another-name of the MAC address in the static blacklist.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** This command is not allowed if the MAC address exists in the whitelist.  
One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name. The another-name is null if it is not configured.

**Configuration Examples** The following example configures the device with the source MAC address 0000.0000.0001 to the static blacklist.

```
Hostname(config-wids)# static-blacklist mac-address 0000.0000.0001
```

The following example restores the default setting.

```
Hostname(config-wids)# no static-blacklist mac-address 0000.0000.0001
```

**Related Commands**

Command	Description
N/A	N/A

**Platform Description** N/A

## 1.77 static-blacklist max

Use this command to configure the maximum number of static blacklist members.

Use the **no** form of this command to restore the default setting.

**static-blacklist max** *number*

**no static-blacklist max**

**Parameter Description**

Parameter	Description
<i>number</i>	Specifies the maximum number of static blacklist members in the range from 1 to 2048.

**Defaults** The default is 1024.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of static blacklist members to 1000.

**Examples**

```
Hostname(config-wids)# static-blacklist max 1000
```

The following example restores the default setting.

```
Hostname(config-wids)#no static-blacklist max
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.78 user-isolation enable

Use this command to enable user isolation on the AP or AC. Use the **no** form of this command to disable this function.

**user-isolation { ap | ssid-ap } enable**

**no user-isolation { ap | ssid-ap } enable**

**Parameter  
Description**

Parameter	Description
<b>ap</b>	Enables user isolation on the AP.
<b>ssid-ap</b>	Enables SSID-based user isolation on the AP.

**Defaults**

This function is disabled by default.

**Command  
Mode**

WIDS configuration mode

**Usage Guide**

N/A

**Configuration**

The following example enables user isolation on an AP.

**Examples**

```
Hostname(config-wids)# user-isolation ap enable
```

The following example restores the default setting.

```
Hostname(config-wids)# no user-isolation ap enable
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform**

N/A

**Description**

## 1.79 user-isolation permit-mac

Use this command to configure a permissible MAC address list for user isolation. Use the **no** form of this command to delete a permissible MAC address.

**user-isolation permit-mac mac *H.H.H***

**no user-isolation permit-mac mac *H.H.H***

Parameter	Parameter	Description
Description	<i>H.H.H</i>	The permissible MAC address list for user isolation.

**Defaults** N/A

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets MAC 0000.0000.0001 as a permissible MAC for user isolation.

```
Hostname(config-wids)# user-isolation permit-mac 0000.0000.0001
```

The following example deletes MAC 0000.0000.0001 from the permissible MAC address list.

```
Hostname(config-wids)# no user-isolation permit-mac 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show wids user-isolation permit-mac** command to view the configured permissible MAC address list for user isolation.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.80 user-isolation permit-mac max

Use this command to configure the maximum number of a permissible MAC address list for user isolation. Use the **no** form of this command to restore the default setting.

**user-isolation permit-mac max *num***

**no user-isolation permit-mac max**

Parameter Description	Parameter	Description
	<i>num</i>	The maximum number of a permissible MAC address list for user isolation in the range from 1 to 2048.

**Defaults** The default is 1024.

**Command Mode** WIDS configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the maximum number of a permissible MAC address list for user isolation to 100.

```
Hostname(config-wids)# user-isolation permit-mac max 100
```

The following example restores the default setting.

```
Hostname(config-wids)#no user-isolation permit-mac max
```

Related Commands	Command	Description
	N/A	N/A

**Verification** Run the **show running-config** command to show the configuration.

**Notifications** N/A

**Common Errors** N/A

**Platform Description** N/A

### 1.81 whitelist mac-address

Use this command to configure an entry for the whitelist. Use the **no** form of this command to delete the whitelist

**whitelist mac-address** *H.H.H* [ **name** *another-name* ]

**no whitelist mac-address** *H.H.H*

Parameter Description	Parameter	Description
	<i>H.H.H</i>	Indicates you set the device with the source MAC address H.H.H as a whitelist entry.

<i>another-name</i>	The another-name of the MAC address in the whitelist.
---------------------	---

**Defaults** N/A

**Command** WIDS configuration mode

**Mode**

**Usage Guide** One another-name may map to multiple MAC addresses, while one MAC address can map to only one another-name. The another-name is null if it is not configured.

**Configuration** The following example configures the device with the source MAC address 0000.0000.0001 to the whitelist.

**Examples**

```
Hostname(config-wids)# whitelist mac-address 0000.0000.0001
```

The following example deletes the device with the source MAC address 0000.0000.0001 from the whitelist.

```
Hostname(config-wids)# no whitelismac-address 0000.0000.0001
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.82 whitelist max

Use this command to configure the maximum number of whitelists.

Use the **no** form of this command to restore the default setting.

**whitelist max num**

**no whitelist max**

Parameter Description	Parameter	Description
	<i>num</i>	Specifies the maximum number of whitelists in the range from 1 to 2048.

**Defaults** The default is 1024.

**Command** WIDS configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the maximum number of whitelists to 1000.

**Examples**

```
Hostname(config-wids)# whitelist max 1000
```

The following example restores the default setting.

```
Hostname(config-wids)#no whitelist max
```

#### Related Commands

Command	Description
N/A	N/A

**Verification** Run the **show running-config** command to show the configuration.

**Notifications** N/A

**Common Errors** N/A

**Platform  
Description** N/A

## 1.83 wids

Use this command to enter the WIDS configuration mode.

**wids**

#### Parameter Description

Parameter	Description
N/A	N/A

**Defaults** N/A

**Command  
Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enters the WIDS configuration mode.

#### Examples

```
Hostname(config)# wids
Hostname(config-wids)#
```

#### Related Commands

Command	Description
N/A	N/A

**Platform  
Description** N/A



# WLAN Security Commands

---

1. AAA Commands
2. RADIUS Commands
3. IEEE 802.1X Commands
4. Web Authentication Commands
5. SCC Commands



# 1 AAA Commands

## 1.1 aaa accounting commands

Use this command to configure NAS command accounting.

Use the **no** form of this command to restore the default setting.

**aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [ *method2...* ]

**no aaa accounting commands** *level* { **default** | *list-name* }

Parameter	Parameter	Description
Description	<i>level</i>	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for command accounting.
	<i>list-name</i>	Name of the command accounting method list, which could be any character strings.
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	<b>none</b>	Does not perform accounting.
	<b>group</b>	Uses the server group for accounting.

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The operating system enables the accounting function after login authentication is enabled. After enabling the accounting function, it sends the command information to the security service. The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

**Configuration** The following example enables NAS command accounting.

**Examples**

```
Hostname(config)# aaa accounting commands 15 default start-stop group server
```

Related	Command	Description
Commands	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa authentication</b>	Defines AAA authentication.
	<b>accounting commands</b>	Applies the accounting commands to the terminal line.

**Platform** N/A

**Description**

## 1.2 aaa accounting exec

Use this command to enable NAS access accounting.

Use the **no** form of this command to restore the default setting.

**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [ *method2...*]

**no aaa accounting exec** { **default** | *list-name* }

Parameter	Parameter	Description
<b>Description</b>	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
	<i>list-name</i>	Name of the Exec accounting method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>none</b>	Does not perform accounting.
	<b>group</b>	Uses the server group for accounting, the RADIUS group is supported.

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The operating system enables the exec accounting function after login authentication is enabled. After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either.

The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.

**Configuration** The following example enables NAS access accounting.

**Examples**

```
Hostname(config)# aaa accounting network start-stop group radius
```

Related	Command	Description
<b>Commands</b>	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa authentication</b>	Defines AAA authentication.
	<b>accounting commands</b>	Applies the Exec accounting to the terminal line.

**Platform** N/A

**Description**

## 1.3 aaa accounting network

Use this command to enable network access accounting.

Use the **no** form of this command to restore the default setting.

**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [ *method2..* ]

**no aaa accounting network** { **default** | *list-name* }

Parameter	Parameter	Description
<b>Description</b>	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for Network accounting.
	<i>list-name</i>	Name of the accounting method list
	<b>start-stop</b>	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
	<i>method</i>	A method list includes up to four methods.
	<b>none</b>	Does not perform accounting.
	<b>group</b>	Uses the server group for accounting, the RADIUS server group is supported.

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The operating system performs accounting of user activities by sending record attributes to the security server. Use the **start-stop** keyword to set the user accounting option.

**Configuration** The following example enables network access accounting.

**Examples**

```
Hostname(config)# aaa accounting network start-stop group radius
```

Related	Command	Description
<b>Commands</b>	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa authorization network</b>	Defines a network authorization method list.
	<b>aaa authentication</b>	Defines AAA authentication.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.4 aaa accounting start-fail

Use this command to configure a policy for accounting-start failures.

Use the **no** form of this command to restore the default setting.

**aaa accounting start-fail { online | offline }**

**no aaa accounting start-fail**

Parameter Description	Parameter	Description
	<b>online</b>	Sets the accounting start failure policy to online.
	<b>offline</b>	Sets the accounting start failure policy to offline.

**Defaults** No accounting-start failure policy is configured.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure an accounting-start failure policy.

**Configuration Examples** The following examples sets the policy to **offline**, namely, disconnecting the users who fail to start accounting.  
 Hostname(config)# aaa accounting start-fail offline

**Verification** Run the **show running-config** command to check the configuration.

**Prompt** -

**Common Errors** -

**Platform Description** -

## 1.5 aaa accounting update

Use this command to enable the accounting update function.

Use the **no** form of this command to restore the default setting.

**aaa accounting update**

**no aaa accounting update**

**Parameter** N/A

**Description**

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

**Configuration** The following example enables the accounting update function.

```

Examples
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update

```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa accounting network</b>	Defines a network accounting method list.

**Platform** N/A  
**Description**

## 1.6 aaa accounting update periodic

Use this command to set the interval of sending the accounting update message.

Use the **no** form of this command to restore the default setting.

**aaa accounting update periodic** *interval*

**no aaa accounting update periodic**

Parameter	Parameter	Description
<b>Description</b>	<i>interval</i>	Interval of sending the accounting update message, in the unit of minutes. The value ranges from 1 to 525600.

**Defaults** The default is 5 minutes.

**Command Mode** Global configuration mode

**Usage Guide** If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.

**Configuration** The following example sets the interval of accounting update to 1 minute.

```

Examples
Hostname(config)# aaa new-model
Hostname(config)# aaa accounting update
Hostname(config)# aaa accounting update periodic 1

```

Related	Command	Description
Commands	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa accounting network</b>	Defines a network accounting method list.

Platform N/A

Description

## 1.7 aaa authentication dot1x

Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list.

Use the **no** form of this command to delete the 802.1x user authentication method list.

**aaa authentication dot1x** { **default** | *list-name* } *method1* [ *method2...*]

**no aaa authentication dot1x** { **default** | *list-name* }

Parameter	Parameter	Description
Description	<b>default</b>	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
	<i>list-name</i>	Name of the 802.1x user authentication method list, which could be any character string
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

Defaults N/A

Command Global configuration mode

Mode

**Usage Guide** If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the **aaa authentication dot1x** command to configure a default or optional method list for 802.1x user authentication.

The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **RDS\_D1X**. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication dot1x rds_d1x group radius local
```

Related	Command	Description
Commands	<b>aaa new-model</b>	Enables the AAA security service.
	<b>dot1x authentication</b>	Associates a specific method list with the 802.1x user.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.8 aaa authentication enable

Use this command to enable AAA Enable authentication and configure the Enable authentication method list.

Use the **no** form of this command to delete the user authentication method list.

**aaa authentication enable default** *method1* [*method2...*]

**no aaa authentication enable default**

Parameter	Parameter	Description
Description	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server groups are supported.
	<b>enable</b>	Enables AAA Enable authentication.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use the **aaa authentication enable** command to configure a default or optional method list for Enable authentication.

The next method can be used for authentication only when the current method does not work.

The Enable authentication function automatically takes effect after configuring the Enable authentication method list.

**Configuration Examples** The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication enable default group radius local
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>enable</b>	Switchover the user level.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.9 aaa authentication general

Use this command in global configuration mode to configure a generic authentication method for 802.1X, web, and iPortal authentication.

Use the **no** form of this command to delete the method list.

**aaa authentication general** { **default** | *list-name* } *method1* [ *method2...* ]

**no aaa authentication general default**

Parameter Description	Parameter	Description
	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> , and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If a device is configured with 802.1X, web, and iPortal authentication or any two among them, which use the same authentication method, run the **aaa authentication general** command to configure a generic authentication method for them. This saves the effort of configuring a method for each authentication mode. If the **aaa authentication general** and **aaa authentication dot1x** commands are both configured, the **aaa authentication dot1x** command takes priority.

**Configuration Examples** The following example defines an AAA general authentication method list. First the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for



authentication.

```
Hostname(config)# aaa authentication general default group radius local
```

**Verification** Run the **show aaa method-list** command to display the generic authentication method list configuration.

**Prompt** 1. If the specified group is not defined on the device, the following prompt will be displayed:

```
%Group XXX is not existed
```

2. If the configured group type does not support the authentication type, the following prompt will be displayed:

```
The authentication does not support this type of group
```

3. If you configure this command repeatedly, the new configuration will overwrite previous configuration.

**Common**

-

**Errors**

**Platform**

-

**Description**

## 1.10 aaa authentication iportal

Use this command to enable AAA Portal Web user authentication.

Use the **no** form of this command to delete the authentication method list.

```
aaa authentication iportal { default | list-name } method1 [ method2...]
```

```
no aaa authentication iportal { default | list-name }
```

**Parameter  
Description**

Parameter	Description
<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
<i>list-name</i>	Name of the user authentication method list, which could be any character strings
<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
<b>local</b>	Uses the local user name database for authentication.
<b>none</b>	Does not perform authentication.
<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** If the AAA Portal Web security service is enabled on the device, users must use AAA for Portal Web authentication negotiation. You must use the **aaa authentication iportal** command to configure a default or optional method list for Portal Web authentication.

**Configuration Examples** The following example defines an AAA Portal Web authentication method list named **rds\_web**. First the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication iportal rds_web group radius local
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>login authentication</b>	Applies the Login authentication method to the terminal lines.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.11 aaa authentication login

Use this command to enable AAA Login authentication and configure the Login authentication method list.

Use the **no** form of this command to delete the authentication method list.

**aaa authentication login** { **default** | *list-name* } *method1* [ *method2..*]

**no aaa authentication login** { **default** | *list-name* }

Parameter Description	Parameter	Description
	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server groups are supported.

**Defaults** N/A

**Command Mode** Global configuration mode

**Mode**

**Usage Guide** If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the **aaa authentication login** command to configure a default or optional method list for Login authentication.

The next method can be used for authentication only when the current method does not work.

You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.

**Configuration Examples** The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication login list-1 group radius local
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>login authentication</b>	Applies the Login authentication method to the terminal lines.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.12 aaa authentication ppp

Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list.

Use the **no** form of this command to delete the authentication method list.

**aaa authentication ppp** { **default** | *list-name* } *method1* [ *method2...*]

**no aaa authentication ppp** { **default** | *list-name* }

Parameter Description	Parameter	Description
	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

**Defaults** N/A

**Command** Global configuration mode  
**Mode**

**Usage Guide** If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the **aaa authentication ppp** command to configure a default or optional method list for PPP user authentication.  
 The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named rds\_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication ppp rds_ppp group radius local
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>ppp authentication</b>	Associates a specific method list with the PPP user.
	<b>username</b>	Defines a local user database.

**Platform** N/A  
**Description**

## 1.13 aaa authentication sslvpn

Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list.

Use the **no** form of this command to delete the authentication method list.

**aaa authentication sslvpn** { **default** | *list-name* } *method1* [ *method2...*]

**no aaa authentication sslvpn** { **default** | *list-name* }

Parameter Description	Parameter	Description
	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication.
	<i>list-name</i>	Name of SSL VPN user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Use the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the **aaa authentication sslvpn** command to configure a default or optional method list for user authentication.

The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **rds\_sslvpn** for SSL VPN session. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.14 aaa authentication web-auth

Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.

Use the **no** form of this command to delete the authentication method list.

**aaa authentication web-auth** { **default** | *list-name* } *method1* [ *method2...*]

**no aaa authentication web-auth** { **default** | *list-name* }

Parameter Description	Parameter	Description
	<b>default</b>	When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication.
	<i>list-name</i>	Name of second-generation Web authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>local</b> , <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authentication.
	<b>none</b>	Does not perform authentication.
	<b>group</b>	Uses the server group for authentication. At present, the RADIUS server group is supported.

**Defaults** N/A

**Command** Global configuration mode  
**Mode**

**Usage Guide** If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the **aaa authentication web-auth** command to configure a default or optional method list for user authentication. The next method can be used for authentication only when the current method does not work.

**Configuration Examples** The following example defines an AAA authentication method list named **rds\_web**. In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.

```
Hostname(config)# aaa authentication web-auth rds_web group radius none
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.15 aaa authorization commands

Use this command to authorize the command executed by the user who has logged in the NAS CLI. Use the **no** form of this command to restore the default setting.

**aaa authorization commands** *level* { **default** | *list-name* } *method1* [ *method2...*]

**no aaa authorization commands** *level* { **default** | *list-name* }

Parameter Description	Parameter	Description
	<i>level</i>	Command level to be authorized in the range from 0 to 15
	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for command authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: <b>none</b> and <b>group</b> . One method list can contain up to four methods.
	<b>none</b>	Do not perform authorization.
	<b>group</b>	Uses the server group for authorization.

**Defaults** This function is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** The operating system supports authorization of the commands executed by the users. When the

users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny. It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level.

The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.

**Configuration** The following example uses the server to authorize the level 15 command.

**Examples**

```
Hostname(config)# aaa authorization commands 15 default group server
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>authorization commands</b>	Applies the command authorization for the terminal line.

**Platform** N/A

**Description**

## 1.16 aaa authorization config-commands

Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode).

Use the **no** form of this command to restore the default setting.

**aaa authorization config-commands**

**no aaa authorization config-commands**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the **no** form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.

**Configuration** The following example enables the configuration command authorization function.

**Examples**

```
Hostname(config)# aaa authorization config-commands
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.

<b>aaa authorization commands</b>	Defines the AAA command authorization.
-----------------------------------	--

**Platform** N/A

**Description**

## 1.17 aaa authorization console

Use this command to authorize the commands of the users who have logged in the console.

Use the **no** form of this command to restore the default setting.

**aaa authorization console**

**no aaa authorization console**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** The operating system can identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.

**Configuration Examples** The following example enables the aaa authorization console function.

```
Hostname(config)# aaa authorization console
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa authorization commands</b>	Defines the AAA command authorization.
	<b>authorization commands</b>	Applies the command authorization to the terminal line.

**Platform** N/A

**Description**

## 1.18 aaa authorization exec

Use this command to authorize the users logged in the NAS CLI and assign the authority level.

Use the **no** form of this command to restore the default setting.

**aaa authorization exec** { **default** | *list-name* } *method1* [ *method2...* ]

**no aaa authorization exec** { **default** | *list-name* }



Parameter	Parameter	Description
Description	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	<b>local</b>	Uses the local user name database for authorization.
	<b>none</b>	Does not perform authorization.
	<b>group</b>	Uses the server group for authorization. At present, the RADIUS server group is supported.

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The **aaa authorization exec** function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the **aaa authorization exec**. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.

**Configuration** The following example uses the RADIUS server to authorize Exec.

**Examples**

```
Hostname(config)# aaa authorization exec default group radius
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>authorization exec</b>	Applies the command authorization to the terminal line.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.19 aaa authorization network

Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network.

Use the **no** form of this command to restore the default setting.

**aaa authorization network** { **default** | *list-name* } *method1* [ *method2...* ]

**no aaa authorization network** { **default** | *list-name* }

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	<b>default</b>	When this parameter is used, the following defined method list is used as the default method for Network authorization.
	<i>method</i>	It must be one of the keywords: none and group. One method list can contain up to four methods.
	<b>none</b>	Does not perform authorization.
	<b>group</b>	Uses the server group for authorization. At present, the RADIUS server group is supported.

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** RGOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically.

Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used.

The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.

**Configuration** The following example uses the RADIUS server to authorize network services.

**Examples**

```
Hostname(config)# aaa authorization network default group radius
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>aaa new-model</b>
	<b>aaa accounting</b>	Defines AAA accounting.
	<b>aaa authentication</b>	Defines AAA authentication.
	<b>username</b>	Defines a local user database.

**Platform** N/A

**Description**

## 1.20 aaa domain

Use this command to configure the domain attributes.

Use the **no** form of this command to restore the default setting.

**aaa domain** { **default** | *domain-name* }

**no aaa domain** { **default** | *domain-name* }

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
------------------	------------------	--------------------

<b>Description</b>	<b>default</b>	Uses this parameter to configure the default domain.
	<i>domain-name</i>	The name of the specified domain

**Defaults** No domain is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to configure the domain-name-based AAA service. The **default** is to configure the default domain. That is the method list used by the network device if the users are without domain information. The *domain-name* is the specified domain name, if the users are with this *domain name*, the method lists associated with this domain are used. At present, the system can configure up to 32 domains.

**Configuration** The following example configures the domain name.

**Examples**

```

Hostname(config)# aaa domain host.com
Hostname(config-aaa-domain)#

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>aaa new-model</b>
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
	<b>show aaa domain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.21 aaa domain enable

Use this command to enable domain-name-based AAA service.

Use the **no** form of this command to restore the default setting.

**aaa domain enable**

**no aaa domain enable**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	N/A	N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** To perform the domain-name-based AAA service configuration, enable this service. If there are authenticated users on the device, enabling or disabling this function may cause an

accounting failure. Restore accounting service through either of the following methods:

1. Run the **clear dot1x user all** command to trigger a new authentication for 802.1X authentication users.
2. Run the **clear web-auth user all** command to disconnect web users, who will initiate an authentication request later.

**Configuration** The following example enables the domain-name-based AAA service.

**Examples**

```

Hostname(config)# aaa domain enable
Accounts of authenticated users are affected, need to clear users.
    
```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>show aaa doamain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.22 aaa heartbeat enable

AAA heartbeat detection is enabled by default. Use this command to enable AAA heartbeat detection to check whether the peer end is available.

Use the **no** form of this command to disable AAA heartbeat detection.

**aaa heartbeat enable**  
**no aaa heartbeat enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** AAA heartbeat detection is enabled.

**Command Mode** Global configuration mode

**Usage Guide** AAA heartbeat detection is enabled by default. AAA heartbeat is supported by only front-end components including RADIUS and 802.1X.

**Configuration** The following example disables AAA heartbeat detection.

**Examples**

```

Hostname(config)# no aaa heartbeat enable
    
```

**Verification** Run the **show running** command to display the domain configuration.

**Prompt** -

**Common**

-

**Platform**

-

## 1.23 aaa local authentication attempts

Use this command to set login attempt times.

**aaa local authentication attempts** *max-attempts*

Parameter	Parameter	Description
Description	<i>max-attempts</i>	In the range from 1 to 2,147,483,647.

**Defaults** The default is 3.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to configure login attempt times.

**Configuration Examples** The following example sets login attempt times to 6.

```

Hostname# configure terminal
Hostname(config)# aaa local authentication attempts 6

```

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current configuration of the switch.
	<b>show aaa lockout</b>	Displays the lockout configuration parameter of current login.

**Platform** N/A

**Description**

## 1.24 aaa local authentication lockout-time

Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.

**aaa local authentication lockout-time** *lockout-time*

Parameter	Parameter	Description
Description	<i>lockout-time</i>	In the range from 1 to 43,200 in the unit of minutes

**Defaults** The default is 15 minutes.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.

**Configuration** The following example sets the lockout-time period to 5 minutes.

**Examples**

```
Hostname# configure terminal
Hostname(config)# aaa local authentication lockout-time 5
```

Related	Command	Description
Commands	<b>show running-config</b>	Displays the current configuration of the switch.
	<b>show aaa lockout</b>	Displays the lockout configuration parameter of current login.

**Platform** N/A

**Description**

## 1.25 aaa log enable

Use this command to enable the system to print the syslog informing AAA authentication success.

Use the **no** form of this command to restore the default setting.

**aaa log enable**

**no aaa log enable**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to enable the system to print the syslog informing aaa authentication success.

**Configuration** The following example disables the system to print the syslog informing aaa authentication success.

**Examples**

```
Hostname(config)# no aaa log enable
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.26 aaa log rate-limit

Use this command to set the rate of printing the syslog informing AAA authentication success.

Use the **no** form of this command to restore the default printing rate.

**aaa log rate-limit** *num*

**no aaa log rate-limit**

Parameter	Parameter	Description
Description	<i>num</i>	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.

**Defaults** The default is 5.

**Command Mode** Global configuration mode

**Usage Guide** Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.

**Configuration Examples** The following example sets the rate of printing the syslog informing AAA authentication success to 10.

```
Hostname(config)# aaa log rate-limit 10
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.27 aaa new-model

Use this command to enable the AAA security service.

Use the **no** form of this command to restore the default setting.

**aaa new-model**

**no aaa new-model**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.

**Configuration** The following example enables the AAA security service.

**Examples**

```
Hostname(config)# aaa new-model
```

**Related****Commands**

Command	Description
<b>aaa authentication</b>	Defines a user authentication method list.
<b>aaa authorization</b>	Defines a user authorization method list.
<b>aaa accounting</b>	Defines a user accounting method list.

**Platform** N/A

**Description**

## 1.28 access-limit

Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users.

Use the **no** form of this command to restore the default setting.

**access-limit** *num*

**no access-limit**

**Parameter****Description**

Parameter	Description
<i>num</i>	The number used for the user limitation is only valid for the IEEE802.1 users. The value ranges from 1 to 1024.

**Defaults**

By default, no number of users is limited.

**Command**

Domain configuration mode

**Mode****Usage Guide**

This command limits the number of users for the domain.

**Configuration**

The following example sets the number of users to 20 for the domain named hostname.com.

**Examples**

```
Hostname(config)# aaa domain hostname.com
Hostname(config-aaa-domain)# access-limit 2
```

**Related****Commands**

Command	Description
<b>aaa new-model</b>	Enables the AAA security service.
<b>aaa domain enable</b>	Switchover the user level.
<b>show aaa domain</b>	Defines a local user database.



**Platform** N/A

**Description**

## 1.29 accounting network

Use this command to configure the Network accounting list.

Use the **no** form of this command to restore the default setting.

**accounting network** { **default** | *list-name* }

**no accounting network**

Parameter	Parameter	Description
<b>Description</b>	<b>default</b>	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the network accounting list

**Defaults** With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.

**Command** Domain configuration mode

**Mode**

**Usage Guide** Use this command to configure the Network accounting method list for the specified domain.

**Configuration** The following example sets the Network accounting method list for the specified domain.

**Examples**

```

Hostname(config)# aaa domain ruijie.com
Hostname(config-aaa-domain)# accounting network default

```

Related	Command	Description
<b>Commands</b>	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
	<b>show aaa domain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.30 authentication

Use this command to configure the IEEE802.1X, PPP, or web authentication list.

Use the **no** form of this command to restore the default setting.

**authentication** { **dot1x** | **ppp** | **web-auth** } { **default** | *list-name* }

**no authentication** { **dot1x** | **ppp** | **web-auth** }

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	<b>dot1x</b>	Specifies the 802.1X authentication method list.
	<b>ppp</b>	Specifies the PPP authentication method list.
	<b>web-auth</b>	Specifies the web authentication method list.
	<b>default</b>	Specifies the default authentication method list.
	<i>list-name</i>	The name of the specified method list

**Defaults** With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

**Command** Domain configuration mode

**Mode**

**Usage Guide** Specify an IEEE802.1X, PPP, or web authentication method list for the domain.

**Configuration** The following example sets an IEEE802.1x authentication method list for the specified domain.

**Examples**

```

Hostname(config)# aaa domain hostname.com
Hostname(config-aaa-domain)# authentication dot1x default

```

<b>Related</b>	<b>Command</b>	<b>Description</b>
<b>Commands</b>	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
	<b>show aaa domain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.31 authorization network

Use this command to configure the Network authorization list.

Use the **no** form of this command to restore the default setting.

**authorization network** { **default** | *list-name* }

**no authorization network**

<b>Parameter</b>	<b>Parameter</b>	<b>Description</b>
<b>Description</b>	<b>default</b>	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the specified method list

**Defaults** With no method list specified, if users send the request, the device will attempt to specify the default method list for users.

**Command** Domain configuration mode

**Mode**

**Usage Guide**

**Configuration** The following example sets an authorization method list for the specified domain.

**Examples**

```

Hostname(config)# aaa domain ruijie.com
Hostname(config-aaa-domain)# authorization network default

```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
	<b>show aaa domain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.32 clear aaa local user logout

Use this command to clear the logout user list.

**clear aaa local user logout { all | user-name word }**

Parameter Description	Parameter	Description
	<b>all</b>	Indicates all locked users.
	<b>user-name word</b>	Indicates the ID of the locked User.

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear all the user lists or a specified user list.

**Configuration** The following example clears the logout user list.

**Examples**

```

Hostname(config)# clear aaa local user logout all

```

Related Commands	Command	Description
	<b>show running-config</b>	Displays the current configuration of the switch.
	<b>show aaa logout</b>	Displays the logout configuration parameter of current login.

**Platform** N/A

**Description**

## 1.33 show aaa accounting update

Use this command to display the accounting update information.

**show aaa accounting update**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the accounting update interval and whether the accounting update is enabled.

**Configuration** The following example displays the accounting update information.

**Examples** Hostname# show aaa accounting update

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.

**Platform** N/A

**Description**

## 1.34 show aaa domain

Use this command to display all current domain information.

**show aaa domain [ default | domain-name ]**

Parameter	Parameter	Description
Description	default	Displays the default domain.
	domain-name	Displays the specified domain.

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** If no domain-name is specified, all domain information will be displayed.

**Configuration** The following example displays the domain named domain.com.

**Examples** Hostname(config)# show aaa domain domain.com  
 =====Domain domain.com=====  
 State: Active

```

Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
authentication dot1x default

```

Related Commands	Command	Description
	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.

**Platform** N/A

**Description**

## 1.35 show aaa lockout

Use this command to display the lockout configuration.

**show aaa lockout**

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the lockout configuration.

**Configuration Examples** The following example displays the lockout configuration.

```

Hostname# show aaa lockout
Lock tries:    3
Lock timeout: 15 minutes

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.36 show aaa group

Use this command to display all the server groups configured for AAA.

**show aaa group**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following command displays all the server groups.

**Examples**

```

Hostname# show aaa group
Type      Reference Name
-----
radius    1          radius
radius    1          dot1x_group
radius    1          login_group
radius    1          enable_group

```

Related	Command	Description
Commands	aaa group server	Configures the AAA server group.

**Platform** N/A

**Description**

## 1.37 show aaa method-list

Use this command to display all AAA method lists.

**show aaa method-list**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display all AAA method lists.

**Configuration** The following example displays the AAA method list.

**Examples**

```

Hostname# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorization network default group radius
    
```

**Related Commands**

Command	Description
<b>aaa authentication</b>	Defines a user authentication method list
<b>aaa authorization</b>	Defines a user authorization method list
<b>aaa accounting</b>	Defines a user accounting method list

**Platform** N/A  
**Description**

### 1.38 show aaa user

Use this command to display AAA user information.

```
show aaa user { all | lockout | by-id session-id | by-name user-name }
```

**Parameter Description**

Parameter	Description
<b>all</b>	Displays all AAA user information.
<b>lockout</b>	Displays the locked AAA user information.
<b>by-id</b> <i>session-id</i>	Displays the information of the AAA user that with a specified session ID.
<b>by-name</b> <i>user-name</i>	Displays the information of the AAA user with a specified user name.

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display AAA user information.

**Configuration Examples** The following example displays AAA user information.

**Examples**

```
Hostname#show aaa user all
```

```

-----
      Id ----- Name
2345687901      wwxxy
-----

Hostname# show aaa user by-id 2345687901

-----
      Id ----- Name
2345687901      wwxxy
-----

Hostname# show aaa user by-name wwxxy

-----
      Id ----- Name
2345687901      wwxxy
-----

Hostname# show aaa user lockout

Name                Tries      Lock      Timeout (min)
-----
Hostname#
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

### 1.39 state

Use this command to set whether the configured domain is valid.

Use the **no** form of this command to restore the default setting.

**state { block | active }**

**no state**

Parameter Description	Parameter	Description
	<b>block</b>	The configured domain is invalid.
	<b>active</b>	The configured domain is valid.

**Defaults** The default is active.



**Command** Domain configuration mode

**Mode**

**Usage Guide** Use this command to set whether the specified configured domain is valid.

**Configuration** The following example sets the configured domain to be invalid.

**Examples**

```
Hostname(config)# aaa domain hostname.com
Hostname(config-aaa-domain)# state block
```

**Related**

**Commands**

Command	Description
<b>aaa new-model</b>	Enables the AAA security service.
<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
<b>show aaa domain enable</b>	Displays the domain configuration.

**Platform** N/A

**Description**

## 1.40 username-format

Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

Use the **no** form of this command to restore the default setting.

**username-format** { **without-domain** | **with-domain** }

**no username-format**

**Parameter**

**Description**

Parameter	Description
<b>without-domain</b>	Sets the user name without the domain information.
<b>with-domain</b>	Sets the user name with the domain information.

**Defaults** The default is without-domain.

**Command** Domain configuration mode

**Mode**

**Usage Guide** Use this command to configure the user name whether to be with the domain information when the NAS interacts with the servers.

**Configuration** The following example sets the user name without the domain information.

**Examples**

```
Hostname(config)# aaa domain ruijie.com
Hostname(config-aaa-domain)# username-domain without-domain
```

**Related**

Command	Description
---------	-------------

<b>Commands</b>	<b>aaa new-model</b>	Enables the AAA security service.
	<b>aaa domain enable</b>	Enables the domain-name-based AAA service.
	<b>show aaa domain</b>	Displays the domain configuration.

**Platform** N/A

**Description**

# 1 RADIUS Commands

## 1.1 aaa group server radius

Use this command to enter AAA server group configuration mode.

Use the **no** form of this command to restore the default setting.

**aaa group server radius** *name*

**no aaa group server radius** *name*

Parameter Description	Parameter	Description
	<i>name</i>	Server group name. Keywords "radius" is excluded as it is the default RADIUS server group names.

**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to configure a RADIUS AAA server group.

**Configuration** The following example configures a RADIUS AAA server group named ss.

**Examples**

```

Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# end
Hostname# show aaa group
Type      Reference Name
-----
radius    1          radius
radius    1          ss

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.2 ip radius source-interface

Use this command to specify the source IP address for the RADIUS packet.

Use the **no** form of this command to delete the source IP address for the RADIUS packet.

**ip radius source-interface** *interface-name*

**no radius source-interface** *interface-name*

**Parameter  
Description**

Parameter	Description
<i>interface-name</i>	Interface that the source IP address of the RADIUS packet belongs to.

**Defaults**

The source IP address of the RADIUS packet is set by the network layer.

**Command  
mode**

Global configuration mode

**Usage Guide**

In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.

**Configuration  
Examples**

The following example specifies that the RADIUS packet obtains an IP address from the GigabitEthernet 0/1 interface and uses it as the source IP address of the RADIUS packet.

```
Hostname(config)# ip radius source-interface gigabitethernet 0/1
```

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS server.
<b>ip address</b>	Configures the IP address of the interface.

**Platform**

N/A

**Description**

## 1.3 radius data-flow-format

Use this command to configure the units of data flows and data packets to be sent to a RADIUS server.

Use the **no** form of this command to restore the default setting.

**radius data-flow-format data { byte | kilo-byte | mega-byte | giga-byte } packet { one-packet | kilo-packet | mega-packet | giga-packet }**

**Parameter  
Description**

Parameter	Description
<b>byte</b>	Sets the unit of data flows to bytes.
<b>kilo-byte</b>	Sets the unit of data flows to kilobytes.
<b>mega-byte</b>	Sets the unit of data flows to megabytes.
<b>giga-byte</b>	Sets the unit of data flows to gigabytes.

<b>one-packet</b>	Sets the unit of data packets to packets.
<b>kilo-packet</b>	Sets the unit of data packets to kilo-packets.
<b>mega-packet</b>	Sets the unit of data packets to mega-packets.
<b>giga-packet</b>	Sets the unit of data packets to giga-packets.

**Defaults** The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively.

**Command mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to specify the unit of data flows and data packets as required.

**Configuration** The following example sets the unit of data flows to be sent to a RADIUS server to kilobytes.

**Examples**

```
Hostname(config)# radius data-flow-format data kilo-byte
```

**Verification** Run the **show running-config** command to show the configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.4 radius dscp

Use this command to configure the differentiated services code point (DSCP) value for RADIUS packets. Use the **no** form of this command to restore the default setting.

**radius dscp** *dscp-value*

**no radius dscp**

Parameter Description	Parameter	Description
		<i>dscp-value</i>

**Defaults** The default DSCP value of RADIUS packets is **0**.

**Command mode** Global configuration mode

**Default Level** 14

**Usage Guide** DSCP is in the type of service (ToS) field of the IP header and is used to identify the packet transmission priority. A larger DSCP value indicates a higher packet priority. The default DSCP value of RADIUS packets is **0**. You can configure the DSCP value for RADIUS packets to change the transmission priority of RADIUS packets.

**Configuration** The following example sets the DSCP value of RADIUS packets to **2**.

**Examples** `Hostname(config)#radius dscp 2`

**Verification** Run the **show running-config** command to show the configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.5 radius vendor-specific extend

Use this command to extend RADIUS not to differentiate the IDs of private vendors.

Use the **no** form of this command to restore the default setting.

**radius vendor-specific extend**

**no radius vendor-specific extend**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Only the private vendor IDs of Ruijie are recognized.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to identify the attributes of all vendor IDs by type.

**Configuration** The following example extends RADIUS so as not to differentiate the IDs of private vendors:

**Examples** `Hostname(config)# radius vendor-specific extend`

Related	Command	Description
---------	---------	-------------

Commands	
<b>radius attribute</b>	Configures vendor type.
<b>radius set qos cos</b>	Sets the QoS value sent by the RADIUS server as the cos value of the interface.

**Platform** N/A

**Description**

## 1.6 radius vendor-specific attribute support

Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor.

Use the **no** form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.

**radius vendor-specific attribute support { cisco | huawei | ms }**

**no radius vendor-specific attribute support { cisco | huawei | ms }**

Parameter Description	Parameter	Description
	<b>cisco</b>	Indicates the private attribute of Cisco.
	<b>huawei</b>	Indicates the private attribute of Huawei.
	<b>ms</b>	Indicates the private attribute of Microsoft.

**Defaults** By default, RADIUS accounting request packets carry the private attribute of a specified vendor.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.

**Configuration Examples** 1. The following example configures that RADIUS accounting request packets carry the private attribute of Huawei.

```
Hostname(config)# radius vendor-specific attribute support huawei
```

2. The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei.

```
Hostname(config)# no radius vendor-specific attribute support huawei
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.7 radius-server accounting-on enable

Use this command to enable the function of sending accounting-on packets upon device restart. Use the **no** form of this command to disable this feature.

**radius-server accounting-on enable**

**no radius-server accounting-on enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** The function of sending accounting-on packets upon device restart is enabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** The accounting-on function is used to notify a RADIUS server of the device restart. After the device is restarted, online users are forced offline. However, the RADIUS server does not perceive the device restart and does not log off the users. As a result, the users encounter an exception when initiating re-authentication. Therefore, it is necessary to enable the accounting-on function.

**Configuration Examples** The following example enables the function of sending accounting-on packets upon device restart.

```
Hostname(config)# no radius-server accounting-on enable
```

**Verification** Run the **show running-config** command to show the configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.8 radius-server account update retransmit

Use this command to configure accounting update packet retransmission for the second generation Web authentication user.



Use the **no** form of this command to restore the default setting.

**radius-server account update retransmit**

**no radius-server account update retransmit**

Parameter Description	Parameter	Description
		N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.

**Configuration Examples** The following example configures accounting update packet retransmission for the second generation Web authentication user.

```
Hostname(config)#radius-server account update retransmit
```

Related Commands	Command	Description
		N/A

**Platform Description** N/A

## 1.9 radius-server attribute 31

Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute.

Use the **no** form of this command to restore the default setting.

**radius-server attribute 31 mac format { ietf | normal | unformatted | dot-split | colon-split | hyphen-split } [ mode1 | mode2 ] [ lowercase | uppercase ]**

**no radius-server attribute 31 mac format**

Parameter Description	Parameter	Description
		<b>ietf</b>
	<b>normal</b>	Normal format representing the MAC address. '.' is used as the separator. For example: 00d0.f833.22ac.
	<b>unformatted</b>	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.

<b>dot-split</b>	Format representing the MAC address. '.' is used as the separator. This parameter should be configured with <b>mode1</b> or <b>mode2</b> .
<b>colon-split</b>	Format representing the MAC address. ':' is used as the separator. This parameter should be configured with <b>mode1</b> or <b>mode2</b> .
<b>hyphen-split</b>	Format representing the MAC address. '-' is used as the separator. This parameter should be configured with <b>mode1</b> or <b>mode2</b> .
<b>mode1</b>	Format representing the MAC address. Four characters make up one group. This parameter should be configured with <b>dot-split</b> , <b>colon-split</b> , or <b>hyphen-split</b> . For example: 00D0.F833.22AC, 00D0:F833:22AC, and 00D0-F833-22AC.
<b>mode2</b>	Format representing the MAC address. Two characters make up one group. This parameter should be configured with <b>dot-split</b> , <b>colon-split</b> , or <b>hyphen-split</b> . For example: 00.D0.F8.33.22.AC, 00:D0:F8:33:22:AC, and 00-D0-F8-33-22-AC
<b>lowercase</b>	Lowercase letters to be used in the MAC address.
<b>uppercase</b>	Uppercase letters to be used in the MAC address.

**Defaults** The default format is unformatted.

**Command** Global configuration mode

**Mode**

**Usage Guide** Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.

**Configuration** The following example defines the RADIUS Calling-Station-ID attribute as IETF format.

**Examples**

```
Hostname(config)# radius-server attribute 31 mac format ietf
```

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS server.

**Platform** N/A

**Description**

## 1.10 radius-server attribute class

Use this command to analyze the flow control value of the RADIUS CLASS attributes.

Use the **no** form of this command to restore the default setting.

```
radius-server attribute class user-flow-control { format-16bytes | format-32bytes | unit bit/s |  
unit byte/s }
```

```
no radius-server attribute class user-flow-control
```

Parameter Description	Parameter	Description
	<b>user-flow-control</b>	Analyzes flow control value in the CLASS attribute.
	<b>format-16bytes</b>	Sets the format of flow control value to 16 bytes.
	<b>format-32bytes</b>	Sets the format of flow control value to 32 bytes.
	<b>unit bit/s</b>	Sets the format of the rate limit value parsed from the <b>class</b> attribute to bps.
	<b>unit byte/s</b>	Sets the format of the rate limit value parsed from the <b>class</b> attribute to bytes/s.

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is required if the server pushes the flow control value through the CLASS attribute.

**Configuration Examples** The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes.

```
Hostname(config)#radius-server attribute class user-flow-control
format-32bytes
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.11 radius-server dead-criteria

Use this command to configure criteria on a device to determine that the RADIUS server is unreachable.

Use the **no** form of this command to restore the default setting.

**radius-server dead-criteria** { **time** *seconds* [ **tries** *number* ] | **tries** *number* }

**no radius-server dead-criteria** { **time** [ **tries** ] | **tries** }

Parameter Description	Parameter	Description
	<b>time</b> <i>seconds</i>	Configures the timeout value. If the device does not receive a correct response packet from the RADIUS server within the specified time, the RADIUS server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.

<b>tries</b> <i>number</i>	Configures the successive timeout times. When sending a request from the device to the RADIUS server times out for the specified times, the device considers that the RADIUS server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.
----------------------------	---

**Defaults** The default **time** *seconds* is 60 and **tries** *number* is 10.

**Command** Global configuration mode

**Mode**

**Usage Guide** If a RADIUS server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.

**Configuration** The following example sets the timeout to 120 seconds and timeout times to 20.

**Examples**

```
Hostname(config)# radius-server dead-criteria time 120 tries 20
```

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server deadtime</b>	Defines the duration when a device stops sending any requests to an unreachable RADIUS server.
<b>radius-server timeout</b>	Defines the timeout for the packet re-transmission.

**Platform** N/A

**Description**

## 1.12 radius-server deadtime

Use this command to configure the duration when a device stops sending any requests to an unreachable RADIUS server.

Use the **no** form of this command to restore the default setting.

**radius-server deadtime** *minutes*

**no radius-server deadtime**

**Parameter  
Description**

Parameter	Description
<i>minutes</i>	Defines the duration in minutes when the device stops sending any requests to the unreachable RADIUS server. The value is in the range from 1 to 1,440 in the unit of minutes.

**Defaults** The default value of *minutes* is 5.

**Command** Global configuration mode

**Mode**

**Usage Guide** If active RADIUS server detection is enabled on the device, the time parameter of this command does not take effect on the RADIUS server. Otherwise, the RADIUS server becomes reachable when the duration set by this command is shorter than the unreachable time.

**Configuration** The following example sets the duration when the device stops sending requests to 1 minute.

**Examples**

```
Hostname(config)# radius-server deadtime 1
```

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server dead-criteria</b>	Defines the criteria to determine that a RADIUS server is unreachable.

**Platform** N/A

**Description**

## 1.13 radius-server host

Use this command to specify a RADIUS security server host.

Use the **no** form of this command to restore the default setting.

**radius-server host** { *ipv4-address* | *ipv6-address* } [ **auth-port** *port-number* ] [ **acct-port** *port-number* ] [ **test username** *name* [ **ignore-auth-port** ] [ **ignore-acct-port** ] [ **idle-time** *time* ] ] [ **key** [ **0** | **7** ] *text-string* ]

**no radius-server host** { *ipv4-address* | *ipv6-address* }

**Parameter  
Description**

Parameter	Description
<b>oob</b>	Specifies an MGMT port as the source port.
<i>ipv4-address</i>	IPv6 address of the RADIUS security server host.
<i>ipv6-address</i>	IPv4 address of the RADIUS security server host.
<i>auth-port</i>	UDP port used for RADIUS authentication.
<i>port-number</i>	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
<i>acct-port</i>	UDP port used for RADIUS accounting.
<i>port-number</i>	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
<b>test username</b> <i>name</i>	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
<b>idle-time</b> <i>time</i>	(Optional) Sets the interval of sending the test packets to the

	reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
<b>ignore-auth-port</b>	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
<b>ignore-acct-port</b>	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
<b>key [ 0   7 ] <i>text-string</i></b>	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.

**Defaults** No RADIUS host is specified by default.

**Command Mode** Global configuration mode

**Usage Guide** In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the **radius-server host** command.

**Configuration** The following example defines a RADIUS security server host:

**Examples**

```
Hostname(config)# radius-server host 192.168.12.1
```

The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection:

```
Hostname(config)# radius-server host 192.168.100.1 test username viven
idle-time 60 ignore-acct-port
```

The following example defines a RADIUS security server host in the IPv6 environment

```
Hostname(config)# radius-server host 3000::100
```

**Related Commands**

Command	Description
<b>aaa authentication</b>	Defines the AAA authentication method list
<b>radius-server key</b>	Defines a shared password for the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.

**Platform Description** N/A

## 1.14 radius-server key

Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server.

Use the **no** form of this command to restore the default setting.

**radius-server key** [ 0 | 7 ] *text-string*

**no radius-server key**

### Parameter Description

Parameter	Description
<i>text-string</i>	Text of the shared password
0   7	Password encryption type. 0: no encryption; 7: Simply-encrypted.

**Defaults** No shared password is specified by default.

### Command

**Mode** Global configuration mode.

**Usage Guide** A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.

**Configuration** The following example defines the shared password **aaa** for the RADIUS security server:

**Examples**

```
Hostname(config)# radius-server key aaa
```

### Related Commands

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server timeout</b>	Defines the timeout for the RADIUS packet.

**Platform** N/A

### Description

## 1.15 radius-server retransmit

Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond.

Use the **no** form of this command to restore the default setting.

**radius-server retransmit** *retries*

**no radius-server retransmit**

Parameter Description	Parameter	Description
	<i>retries</i>	Packet retransmission count before the device confirms that a RADIUS server is unreachable. The value range is from 0 to 100 and the value <b>0</b> indicates no retransmission.

**Defaults** The default is 3.

**Command Mode** Global configuration mode.

**Usage Guide** AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.

**Configuration Examples** The following example sets the number of retransmissions to 4.

```
Hostname(config)# radius-server retransmit 4
```

Related Commands	Command	Description
	<b>radius-server host</b>	Defines the RADIUS security server.
	<b>radius-server key</b>	Defines a shared password for the RADIUS server.
	<b>radius-server timeout</b>	Defines the timeout for the RADIUS packet.

**Platform Description** N/A

## 1.16 radius-server source-port

Use this command to configure the source port to send RADIUS packets.

Use the **no** form of this command to restore the default setting.

**radius-server source-port** *port*

**no radius-server source-port**

Parameter Description	Parameter	Description
	<i>port</i>	The port ID, in the range from 1 to 65535.

**Defaults** The default is a random number.



**Command** Global configuration mode

**Mode**

**Usage Guide** The source port is random by default. This command is used to specify a source port.

**Configuration** The following example configures source port 10000 to send RADIUS packets.

**Examples**

```
Hostname(config)# radius-server source-port 10000
```

**Related  
Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.17 radius-server timeout

Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet.

Use the **no** form of this command to restore the default setting.

**radius-server timeout** *seconds*

**no radius-server timeout**

**Parameter  
Description**

Parameter	Description
<i>seconds</i>	Timeout in the range from 1 to 1,000 in the unit of seconds.

**Defaults** The default is 5 seconds.

**Command**

**Mode** Global configuration mode

**Usage Guide** This command is used to change the timeout of packet retransmission.

**Configuration** The following example sets the timeout to 10 seconds.

**Examples**

```
Hostname(config)# radius-server timeout 10
```

**Related  
Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of the RADIUS packet retransmissions.

<b>radius-server key</b>	Defines a shared password for the RADIUS server.
--------------------------	--

**Platform** N/A

**Description**

## 1.18 radius-server authentication attribute

Use this command to configure whether authentication request packets carry specified attributes. Use the **no** form of this command to remove the setting. Use the **default** form of this command to restore the default setting.

**radius-server authentication attribute** *type* { **package** | **unpackage** }

**no radius-server authentication attribute** *type* { **package** | **unpackage** }

**default radius-server authentication attribute** *type* { **package** | **unpackage** }

**Parameter  
Description**

Parameter	Description
<i>type</i>	Type of a RADIUS attribute. The value range is from 1 to 255.
<b>package</b>	Indicates that RADIUS authentication request packets carry specified attributes.
<b>unpackage</b>	Indicates that RADIUS authentication request packets do not carry specified attributes.

**Defaults**

The RFC standard stipulates that some attributes are carried in authentication request packets, some attributes are not carried, and the other attributes can either be carried or not. The default configuration follows the RFC stipulation.

**Command  
Mode**

Global configuration mode

**Default Level**

14

**Usage Guide**

Use this command to configure whether RADIUS authentication request packets contain specified attributes.

The configuration must strictly follow the RFC standard, that is, some attributes are carried in authentication request packets while some attributes are not.

Use the **no** or **default** form of this command to restore the default setting.

**Configuration  
Examples**

The following example configures RADIUS authentication request packets not to carry attribute 87.

```
Hostname(config)# radius-server authentication attribute 87 unpackage
```

**Verification**

The RADIUS authentication request packet obtained on the RADIUS server does not contain attribute 87.

**Prompt**

N/A

<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

## 1.19 radius-server account attribute

Use this command to configure whether RADIUS accounting request packets carry specified attributes. Use the **no** or **default** form of this command to restore the default setting.

**radius-server account attribute** *type* { **package** | **unpackage** }

**no radius-server account attribute** *type* { **package** | **unpackage** }

**default radius-server account attribute** *type* { **package** | **unpackage** }

<b>Parameter Description</b>	Parameter	Description
	<i>type</i>	Type of a RADIUS attribute. The value range is from 1 to 255.
	<b>package</b>	Indicates that RADIUS accounting request packets carry specified attributes.
	<b>unpackage</b>	Indicates that RADIUS accounting request packets do not carry specified attributes.

**Defaults** The RFC standard stipulates that some attributes are carried in accounting request packets, some attributes are not carried, and the other attributes can either be carried or not. The default configuration follows the RFC stipulation.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure whether RADIUS accounting request packets contain specified attributes. The configuration must strictly follow the RFC standard, that is, some some attributes are carried in accounting request packets while some attributes are not. Use the **no** or **default** form of this command to restore the default setting.

**Configuration Examples** The following example configures RADIUS accounting request packets not to carry attribute 87.

```
Hostname(config)# radius-server account attribute 87 unpackage
```

**Verification** The RADIUS accounting request packet obtained on the RADIUS server does not contain attribute 87.

<b>Prompt</b>	N/A
<b>Common Errors</b>	N/A
<b>Platform Description</b>	N/A

## 1.20 radius-server authentication vendor

Use this command to configure authentication request packets to carry specified vendor-specific attributes (VSAs). Use the **no** or **default** form of this command to restore the default setting.

**radius-server authentication vendor [ cmcc | microsoft | cisco | hw ] package**

**no radius-server authentication vendor** *vendor\_name* **package**

**default radius-server authentication vendor** *vendor\_name* **package**

### Parameter Description

Parameter	Description
<b>cmcc</b>	Indicates that CMCC VSA is carried.
<b>microsoft</b>	Indicates that Microsoft VSA is carried.
<b>cisco</b>	Indicates that Cisco VSA is carried.
<b>hw</b>	Indicates that Huawei VSA is carried.

**Defaults** No other VSAs are carried in authentication request packets.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure RADIUS authentication request packets to carry specified VSAs.

**Configuration Examples** The following example configures authentication request packets to carry CMCC private attributes.

```
Hostname(config)# radius-server authentication vendor cmcc package
```

**Verification** The RADIUS authentication request packet obtained on the RADIUS server does not contain CMCC VSA.

**Prompt** N/A

**Common Errors** N/A

**Platform**  
**Description** N/A

## 1.21 radius-server account vendor

Use this command to configure accounting request packets to carry specified VSAs. Use the **no** or **default** form of this command to restore the default setting.

**radius-server account vendor** [ **cmcc** | **microsoft** | **cisco** | **hw** ] **package**

**no radius-server account vendor** *vendor\_name* **package**

**default radius-server account vendor** *vendor\_name* **package**

Parameter Description	Parameter	Description
	<b>cmcc</b>	Indicates that CMCC VSA is carried.
	<b>microsoft</b>	Indicates that Microsoft VSA is carried.
	<b>cisco</b>	Indicates that Cisco VSA is carried.
	<b>hw</b>	Indicates that Huawei VSA is carried.

**Defaults** No other VSAs are carried in accounting request packets.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to configure RADIUS accounting request packets to carry specified VSAs.

**Configuration Examples** The following example configures RADIUS accounting request packets to carry CMCC private attributes.

```
Hostname(config)# radius-server account vendor cmcc package
```

**Verification** The RADIUS accounting request packet obtained on the RADIUS server does not contain CMCC VSA.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.22 radius set qos cos

Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface.

Use the **no** form of this command to restore the default setting.

**radius set qos cos**

**no radius set qos cos**

Parameter Description	Parameter	Description
		N/A

**Defaults** Set the QoS value sent by the RADIUS server as the DSCP value.

**Command Mode** Global configuration mode.

#### Usage Guide

**Configuration Examples** The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface:

```
Hostname(config)# radius set qos cos
```

Related Commands	Command	Description
		<b>radius vendor-specific extend</b>

**Platform Description** N/A

## 1.23 radius support cui

Use this command to enable RADIUS to support the cui function.

Use the **no** form of this command to restore the default setting.

**radius support cui**

**no radius support cui**

Parameter Description	Parameter	Description
		N/A

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to enable RADIUS to support the cui function.

**Configuration** The following example enables RADIUS to support the cui function.

**Examples**

```
Hostname(config)# radius support cui
```

**Related Commands**

Command	Description
N/A	N/A

**Platform** N/A

**Description**

## 1.24 server auth-port acct-port

Use this command to add the server of the AAA server group.

Use the **no** form of this command to restore the default setting.

**server** { *ipv4-addr* | *ipv6-addr* } [ **auth-port** *port1* ] [ **acct-port** *port2* ]

**no server** { *ipv4-addr* | *ipv6-addr* } [ **auth-port** *port1* ] [ **acct-port** *port2* ]

**Parameter Description**

Parameter	Description
<i>ip-addr</i>	Server IP address
<i>ipv6-addr</i>	Server IPv6 address
<i>port1</i>	Server authentication port
<i>port2</i>	Server accounting port

**Defaults** No server is configured by default.

**Command Mode** Server group configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively.

```
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Hostname(config-gs-radius)# end
Hostname# show aaa group
Type      Reference Name
-----
radius    1          radius
radius    1          ss
```

Related Commands	Command	Description
		N/A

**Platform** N/A  
**Description**

## 1.25 show radius acct statistics

Use this command to display RADIUS accounting statistics.

**show radius acct statistics**

Parameter Description	Parameter	Description
		N/A

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays RADIUS accounting statistics.

```

Hostname#show radius acct statistics
Accounting Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1813
Msg Round Trip Time..... 0 (msec)
First Requests..... 1
Retry Requests..... 1
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests.....
    
```

Related Commands	Command	Description
		N/A



**Platform** N/A  
**Description**

## 1.26 show radius auth statistics

Use this command to display RADIUS authentication statistics.

**show radius auth statistics**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays RADIUS authentication statistics.

```

Examples
Hostname#show radius auth statistics
Authentication Servers:

Server Index..... 1
Server Address..... 192.168.1.1
Server Port..... 1812
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
    
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.27 show radius group

Use this command to display RADIUS server group configuration.

**show radius group**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode/Privileged EXEC mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays RADIUS server group configuration.

**Examples**

```

Hostname#show radius group
=====Radius group radius=====
Server:192.168.1.1
  Server key:radius-key
  Authentication port:1812
  Accounting port:1813
  State:Active

```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

## 1.28 show radius parameter

Use this command to display global RADIUS server parameters.

**show radius parameter**

Parameter Description	Parameter	Description
	N/A	N/A

<b>Defaults</b>	N/A
<b>Command Mode</b>	Global configuration mode/Privileged EXEC mode/Interface configuration mode
<b>Usage Guide</b>	N/A

**Configuration** The following example displays global RADIUS server parameters.

**Examples**

```

Hostname# show radius parameter
Server Timeout: 5 Seconds
Server Deadtime: 0 Minutes
Server Retries: 3
Server Dead Criteria:
Time: 10 Seconds
Tries: 10

```

<b>Related Commands</b>	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.29 show radius server

Use this command to display the configuration of the RADIUS server.

**show radius server**

<b>Parameter Description</b>	Parameter	Description
	N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode, privileged EXEC mode, interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration of the RADIUS server.

**Examples**

```

Hostname# show radius server
Server IP: 192.168.4.12
Accounting Port: 23
Authen Port: 77

```

```

Test Username:   viven
Test Idle Time:  10 Minutes
Test Ports:      Authen
Server State:    Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:       192.168.4.13
Accounting Port: 45
Authen Port:     74
Test Username:   <Not Configured>
Test Idle Time:  60 Minutes
Test Ports:      Authen and Accounting
Server State:    Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
    
```

**Related Commands**

Command	Description
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.
<b>radius-server timeout</b>	Defines the packet transmission timeout.

**Platform** N/A

**Description**

### 1.30 show radius vendor-specific

Use this command to display the VSA configuration.

**show radius vendor-specific**

Parameter	Parameter	Description
-----------	-----------	-------------

<b>Description</b>	
N/A	N/A

**Defaults** N/A

**Command Mode** Global configuration mode, privileged EXEC mode, interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration of the private vendors.

```

Examples
Hostname# show radius vendor-specific
id      vendor-specific      type-value
-----
1       max-down-rate          1
2       port-priority          2
3       user-ip              3
4       vlan-id              4
5       last-supPLICANT-vers 5
        ion
6       net-ip              6
7       user-name            7
8       password            8
9       file-directory        9
10      file-count           10
11      file-name-0          11
12      file-name-1          12
13      file-name-2          13
14      file-name-3          14
15      file-name-4          15
16      max-up-rate          16
17      current-supPLICANT-version 17
18      flux-max-high32      18
19      flux-max-low32       19
20      proxy-avoid          20
21      dialup-avoid         21
22      ip-privilege         22
23      login-privilege      42
26      ipv6-multicast-addr 79
        ss
27      ipv4-multicast-addr 87
        ss
    
```

<b>Related</b>	<b>Command</b>	<b>Description</b>
----------------	----------------	--------------------

Commands	
<b>radius-server host</b>	Defines the RADIUS security server.
<b>radius-server retransmit</b>	Defines the number of RADIUS packet retransmissions.
<b>radius-server key</b>	Defines a shared password for the RADIUS server.
<b>radius-server timeout</b>	Defines the packet transmission timeout.

**Platform** N/A

**Description**

## 1.31 show radius attribute

Use this command to display the RADIUS attribute.

**show radius attribute**

Parameter Description	Parameter	Description
	-	-

**Command Mode** Global configuration mode, privileged EXEC mode, interface configuration mode

14

**Usage Guide** N/A

**Configuration Examples** The following example displays the RADIUS attribute.

```

Hostname#sh radius attribute
type          implicate
-----
1..... User-Name
2..... User-Password
3..... Chap-Password
4..... NAS-Ip-Addr
5..... Nas-Ip-Port
6..... Service-Type
7..... Framed-Protocol
8..... Frame-Ip-Address
9..... Framed-Ip-Mask
10..... Framed-Routing
11..... Filter-Id
12..... Framed-Mtu

```

13..... Framed-Compress  
14..... Login-Ip-Host  
15..... Login-Service  
16..... Login-Tcp-Port  
18..... Reply-Message  
19..... Callback-Num  
20..... Callback-Id  
22..... Framed-Route  
23..... Framed-IPX-Network  
24..... State  
25..... Class  
26..... Vendor-Specific  
27..... Session-Timeout  
28..... Idle-Timeout  
29..... Termination-Action  
30..... Called-Station-Id  
31..... Calling-Station-Id  
32..... Nas-Id  
33..... Proxy-State  
34..... Login-LAT-Service  
35..... Login-LAT-Node  
36..... Login-LAT-Group  
37..... Framed-AppleTalk-Link  
38..... Framed-AppleTalk-Net  
39..... Framed-AppleTalk-Zone  
40..... Acct-Status-Type  
41..... Acct-Delay-Time  
42..... Acct-Input-Octets  
43..... Acct-Output-Octets  
44..... Acct-Session-Id  
45..... Acct-Authentic  
46..... Acct-Session-Time  
47..... Acct-Input-Packet  
48..... Acct-Output-Packet  
49..... Acct-Terminate-Cause  
50..... Acct-Multi-Session-ID  
51..... Acct-Link-Count  
52..... Acct-Input-Gigawords  
53..... Acct-Output-Gigawords  
60..... Chap-Challenge  
61..... Nas-Port-Type  
62..... Port-Limit  
63..... Login-Lat-Port  
64..... Tunnel-Type

```

65..... Tunnel-Medium-Type
66..... Tunnel-Client-EndPoint
67..... Tunnel-Service-EndPoint
79..... eap msg
80..... Message-Authenticator
81..... group id
85..... Acct-Interim-Interval
87..... Nas-Port-Id
89..... cui
95..... Nas-Ipv6-Addr
96..... Framed-Interface-Id
97..... Framed-Ipv6-Prefix
98..... Login-Ipv6-Host
99..... Framed-Ipv6-Route
100..... Framed-Ipv6-Pool
168..... Framed-Ipv6-Addr
    
```

**Prompt** N/A

**Platform Description** N/A



# 1 IEEE 802.1X Commands

## 1.1 clear dot1x user all

Use this command to clear all the 802.1X authentication users.

**clear dot1x user all**

Parameter	Parameter	Description
Description	N/A	N/A

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear all the 802.1X authentication users.

**Configuration** The following example clears all the 802.1X authentication users.

**Examples**

```
Hostname# clear dot1x user all
```

Related	Command	Description
Commands	N/A	N/A

**Platform** N/A

**Description**

## 1.2 clear dot1x user mac

Use this command to clear 802.1X authentication users according to MAC addresses.

**clear dot1x user mac mac-addr**

Parameter	Parameter	Description
Description	<i>mac-addr</i>	MAC address

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear 802.1X authentication users according to MAC addresses.

**Configuration** The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A.

**Examples**

```
Hostname#clear dot1x user mac 0012.3456.789A
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 1.3 clear dot1x user name

Use this command to clear the 802.1 X authentication users according to the username.

**clear dot1x user name** *name-str*

Parameter	Parameter	Description
<b>Description</b>	<i>name-str</i>	The username of the 802.1X authentication user

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear the 802.1 X authentication users according to the username.

**Configuration** The following example clears the 802.1X authentication user named 802.1X-user.

**Examples**

```
Hostname# clear dot1x user name dot1x-user
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A

**Description**

### 1.4 clear dot1x user ip

Use this command to clear 802.1X authentication users according to IP addresses.

**clear dot1x user ip** *ip-addr*

Parameter	Parameter	Description
<b>Description</b>	<i>ip-addr</i>	IP address

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to clear 802.1X authentication users according to IP addresses.

**Configuration Examples** The following example clears an 802.1X authentication user whose IP address is 11.1.1.1.

```
Hostname# clear dot1x user ip 11.1.1.1
```

**Platform**

N/A

**Description**

## 1.5 default-vlan

Use this command to configure the member VLAN of a VLAN group as the default VLAN upon a 802.1X authentication success. Use the **no** form of this command to remove the configuration.

**default-vlan** *vlan-id*

**no default-vlan** *vlan-id*

Parameter Description	Parameter	Description
	<i>vlan-id</i>	Specifies the member VLAN of a VLAN group as the default VLAN upon a 802.1X authentication success.

**Defaults** No default VLAN is configured.

**Command Mode** VLAN group configuration mode

**Default Level** 14

**Usage Guide** Before configuring the default VLAN, add this VLAN to the VLAN group.  
If the VLAN assignment mode is 802.1X, the authentication server delivers the default VLAN to users upon an authentication success.

**Configuration Examples** The following example sets the default VLAN of VLAN group 1 to VLAN 10.

```
Hostname# configure terminal
Hostname(config)# vlan-group 1
Hostname(config-vlan-group)# default-vlan 10
```

**Verification** Run the **show vlan-group 1** to check the default VLAN configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform** N/A  
**Description**

## 1.6 dot1x accounting

Use this command to configure the accounting list.

**dot1x accounting** *list-name*

Parameter	Parameter	Description
<b>Description</b>	<i>list-name</i>	The name of the accounting list

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If AAA does not adopt 802.1X accounting as the default accounting method. Use this command to configure the 802.1X accounting method.  
 Configuration in WLAN security configuration mode is prior to that in global configuration mode.

**Configuration Examples** The following example configures the accounting list.

```
Hostname(config)# dot1x accounting dot1x-acct
```

Related Commands	Command	Description
	N/A	N/A

**Platform** N/A  
**Description**

## 1.7 dot1x auth-mode

Use this command to specify the 802.1X authentication mode.

**dot1x auth-mode** { eap | chap | pap }

Parameter	Parameter	Description
<b>Description</b>	N/A	N/A

**Defaults** The default is EAP-MD5 authentication mode.

**Command Mode** Global configuration mode

**Usage Guide** The selection of authentication mode depends on the suppliant and portal server.

**Configuration** The following example enables CHAP authentication mode.

**Examples**

```
Hostname(config)# dot1x auth-mode chap
```

Related Commands	Command	Description
	<code>show dot1x</code>	Displays the 802.1X information.

**Platform** N/A

**Description**

## 1.8 dot1x auth-address-table address

Use this command to configure the client device allowed for authentication.

**dot1x auth-address-table address** *mac-addr* **interface** *interface*

Parameter Description	Parameter	Description
	<i>mac-addr</i>	The MAC address of a client device allowed for authentication
	<i>interface</i>	The interface which the client device is connected

**Defaults** N/A

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** This command is used to allow only the client device with the specified MAC address on the specified port to perform IEEE 802.1X authentication.

**Configuration** The example configures the client device allowed for authentication.

**Examples**

```
Hostname(config)# dot1x auth-address-table address 00d0.f800.0cb2 interface fastethernet 0/1
```

**Prompt** N/A

**Platform Description** N/A

## 1.9 dot1x authentication

Use this command to configure the authentication method list.

**dot1x authentication** *list-name*

Parameter	Parameter	Description
Description	<i>list-name</i>	Authentication method list

**Defaults** N/A

**Command Mode** Global configuration mode/WLAN security configuration mode

**Usage Guide** If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.  
Configuration in WLAN security configuration mode is prior to that in global configuration mode.

**Configuration Examples** The following example configures the authentication method list

```
Hostname(config)# dot1x authentication dot1x-authen
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.10 dot1x client-probe enable

Use this command to enable online Ruijie supplicant detection. Use the **no** form of this command to disable this feature.

**dot1x client-probe enable**

**no dot1x client-probe enable**

Parameter Description	Parameter	Description
	N/A	N/A

**Defaults** Online Ruijie supplicant detection is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** You are advised to enable this function when Ruijie supplicant is used.

**Configuration Examples** The following example enables online Ruijie supplicant detection.

```
Hostname(config)# dot1x client-probe enable
```

**Prompt** N/A

**Platform Description** N/A

## 1.11 dot1x dbg-filter

Use this command to enable debug information print for a user with a specified MAC address.  
Use the **no** form of this command to clear the debug information.

**dot1x dbg-filter** *H.H.H*

**no dot1x dbg-filter** *H.H.H*

Parameter	Parameter	Description
<b>Description</b>	<i>H.H.H</i>	The MAC address of a user

**Defaults** Debug information of all authentication users is printed by default.

**Command mode** Global configuration mode

**Usage Guide** Use this command to print the debug information of a specific user. If you want to locate the fault on the network where there are multiple users.

**Configuration Examples** The following example prints the debug information of the device with the specified MAC address.

```
Hostname(config)# dot1x dbg-filter 00d0.f800.0001
```

Related Commands	Command	Description
	N/A	N/A

**Platform Description** N/A

## 1.12 dot1x default-user-limit

Use this command to set the maximum auth-user number on controlled interfaces.  
Use the **no** form of this command to restore the default setting.

**dot1x default-user-limit** *num*

**no dot1x default-user-limit**

Parameter	Parameter	Description
<b>Description</b>	<i>num</i>	The maximum auth-user number allowed by a controlled interface, in the range from 1 to 1,000,000.

- Defaults** By default, there is not a limitation for the auth-user number.
- Command mode** Interface configuration mode
- Usage Guide** This command is used to limit the number of users to be authenticated on a specific port.
- Configuration** The following example sets the maximum auth-user number on a controlled interface.
- Examples**
- ```
Hostname(config-if)# dot1x default-user-limit 10
```

| Related Commands | Command                                                    | Description                                                          |
|------------------|------------------------------------------------------------|----------------------------------------------------------------------|
|                  | <b>show dot1x port-control interface fastEthernet 0/10</b> | Displays the number of users allowed by a specific 802.1X interface. |
|                  | <b>show dot1x port-control interface fastEthernet 0/10</b> | Displays the number of users allowed by a specific 802.1X interface. |

- Platform** N/A
- Description**

## 1.13 dot1x default

Use this command to restore 802.1X configuration to the default setting.

### **dot1x default**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

- Defaults** N/A

- Command Mode** Global configuration mode

- Usage Guide** This command is used to restore 802.1X configuration for quick re-configuration.

- Configuration** The following example restores 802.1X configuration to the default setting.

**Examples**

```
Hostname(config)# dot1x default
```

| Related Commands | Command           | Description                      |
|------------------|-------------------|----------------------------------|
|                  | <b>show dot1x</b> | Displays the 802.1X information. |

- Platform** N/A



**Description**

## 1.14 dot1x encryption only

Use this command to enable the 802.1X authentication for only encryption purpose. WEB authentication functions in place of 802.1X for authentication purpose.

Use the **no** form of this command to restore the default setting.

**dot1x encryption only**

**no dot1x encryption only**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** Use this command to enable the 802.1X authentication for only encryption purpose. WEB authentication functions in place of 802.1X for authentication purpose.

**Configuration Examples** The following example enables the 802.1X authentication for only encryption purpose.

```
Hostname(config-wlansec)# dot1x encryption only
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** This command is supported only on wireless products.

## 1.15 dot1x logging rate-limit

Use this command to set the logging rate-limit.

**dot1x logging rate-limit** *value*

Use this command to restore the default setting.

**no dot1x logging**

| Parameter   | Parameter    | Description                                                                           |
|-------------|--------------|---------------------------------------------------------------------------------------|
| Description | <i>value</i> | Logging rate. The value range is from 0 to 65,535.<br>0: logging rate is not limited. |

**Defaults** The default is 5 logs per second.

|                      |                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Command</b>       | Global configuration mode                                                                                       |
| <b>Mode</b>          |                                                                                                                 |
| <b>Usage Guide</b>   | The default setting is recommended. Lower the limit in case of much online/offline which raises CPU occupation. |
| <b>Configuration</b> | The following example sets the logging rate-limit to 20 logs per second.                                        |
| <b>Examples</b>      | <pre>Hostname(config)# dot1x logging rate-limit 20</pre>                                                        |
| <b>Platform</b>      |                                                                                                                 |
| <b>Description</b>   | This command is supported only on wireless products.                                                            |

## 1.16 dot1x max-req

Use this command to set the maximum attempts of authentication requests.

**dot1x max-req** *num*

|                    | Parameter  | Description                                                          |
|--------------------|------------|----------------------------------------------------------------------|
| <b>Parameter</b>   | <i>num</i> |                                                                      |
| <b>Description</b> |            | Maximum attempts, in the range from 1 to 10. The default value is 3. |

**Defaults** The default is 3.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Use the **show dot1x** command to display the 802.1X configuration.

**Configuration** The following example sets the maximum attempts of authentication requests to 2.

**Examples**

```
Hostname(config)# dot1x max-req 2
```

|                 | Command           | Description                            |
|-----------------|-------------------|----------------------------------------|
| <b>Related</b>  |                   |                                        |
| <b>Commands</b> | <b>show dot1x</b> | Displays the information about 802.1X. |

**Platform** N/A  
**Description**

## 1.17 dot1x multi-account enable

Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.

Use the **no** form of this command to restore the default setting.

**dot1x multi-account enable**

**no dot1x multi-account enable**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use the command to enable the multiple-account authentication if you want to switch the username in the authentication or re-authentication, especially in the windows domain authentication.

**Configuration** The following example enables the multiple-account authentication.

**Examples**

```
Hostname(config)# dot1x multi-account enable
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.18 dot1x port-control auto

Use this command to configure the 802.1X authentication on the port.

Use the **no** form of this command to restore the default setting.

**dot1x port-control auto**

**no dot1x port-control**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode, VXLAN configuration mode

**Usage Guide** Use the **show dot1x** command to display the 802.1X configuration.

**Configuration** The following example configures the 802.1X authentication on the port.

**Examples**

```
Hostname(config-if-GigabitEthernet 0/1)# dot1x port-control auto
```

| Related | Command | Description |
|---------|---------|-------------|
|---------|---------|-------------|

|                 |                   |                                  |
|-----------------|-------------------|----------------------------------|
| <b>Commands</b> | <b>show dot1x</b> | Displays the 802.1X information. |
|-----------------|-------------------|----------------------------------|

**Platform** N/A

**Description**

## 1.19 dot1x offline-detect

Use this command to enable traffic detection.

Use the **no** form of this command to disable this function.

**dot1x offline-detect [ interval *val* | flow *num* | interval *val* flow *num* ]**

**no dot1x offline-detect**

| Parameter Description | Parameter  | Description                                                                                                         |
|-----------------------|------------|---------------------------------------------------------------------------------------------------------------------|
|                       | <i>val</i> | Traffic detection interval in the unit of minutes. The value ranges from 1 to 65,535.<br>The default is 15 minutes. |
|                       | <i>num</i> | Traffic threshold in the unit of KB. The value ranges from 0 to 4,294,967,294.<br>The default is 0 KB.              |

**Defaults** AP: This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** (Optional) Use this command to prevent the device from accounting when a STA has been offline. The traffic detection parameters configured in WLAN security configuration mode are prior to those configured in global configuration mode.

**Configuration Examples** The following example enables traffic detection.

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)#dot1x offline-detect interval 5 flow 20

```

**Platform Description** This command is supported only on wireless products.

## 1.20 dot1x probe-timer interval

Use this command to configure the Ruijie client detection duration.

**dot1x probe-timer interval *time***

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| <i>time</i> | Ruijie client detection duration in seconds. The value range is from 3 to 65,535. |
|-------------|-----------------------------------------------------------------------------------|

**Defaults** 20 seconds

**Command Mode** Global configuration mode

**Usage Guide** The default configuration is recommended.

**Configuration Examples** The following example sets the Ruijie supplicant detection duration to 30 seconds.

```
Hostname(config)# dot1x probe-timer interval 30
```

**Platform Description** N/A

## 1.21 dot1x probe-timer alive

Use this command to configure the Ruijie client detection duration.

**dot1x probe-timer alive** *time*

| Parameter Description | Parameter   | Description                                                                       |
|-----------------------|-------------|-----------------------------------------------------------------------------------|
|                       | <i>time</i> | Ruijie client detection duration in seconds. The value range is from 1 to 65,535. |

**Defaults** 60

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** After a client is authenticated and goes online, if the device fails to receive any detection response from the client within the detection duration, the device considers the client offline.  
The default configuration is recommended.

**Configuration Examples** The following example sets the Ruijie client detection duration to 120 seconds.

```
Hostname(config)# dot1x probe-timer alive 120
```

**Prompt** N/A

**Platform** N/A

**Description**

## 1.22 dot1x private-supplicant-only

Use this command to enable the non-Ruijie supplicant filtering function. Use the **no** form of this command to disable this feature.

**dot1x private-supplicant-only**

**no dot1x private-supplicant-only**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

The non-Ruijie supplicant filtering function is disabled by default.

**Command  
Mode**

Global configuration mode

**Default Level**

15

**Usage Guide**

This function should be configured if Ruijie supplicant must be used for authentication.

**Configuration**

The following example enables the non-Ruijie supplicant filtering function.

**Examples**

```
Hostname(config)# dot1x private-supplicant-only
```

**Prompt**

N/A

**Platform  
Description**

N/A

## 1.23 dot1x pseudo source-mac

Use this command to configure a virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device. Use the **no** form of this command to remove the setting.

**dot1x pseudo source-mac**

**no dot1x pseudo source-mac**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

The source MAC address of IEEE 802.1X packets sent by the device is a virtual MAC address by default.

**Command**

Global configuration mode

**Mode****Default Level** 15

**Usage Guide** Some Ruijie supplicant versions judge whether an access device is a Ruijie device based on the source MAC addresses of EAP packets, so as to implement Ruijie private features. If a device works with such supplicant versions to perform IEEE 802.1X authentication and private features are needed, configure this command on the device.

**Configuration Examples** The following example configures not to use the virtual MAC address as the source MAC address of IEEE 802.1X packets sent by the device.

```
Hostname(config)# dot1x pseudo source-mac
```

**Prompt** N/A**Platform Description** N/A

## 1.24 dot1x redirect

Use this command to enable the 2nd-generation Ruijie supplicant deployment function. Use the **no** form of this command to disable this feature.

**dot1x redirect**

**no dot1x redirect**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The 2nd-generation Ruijie supplicant deployment function is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 15

**Usage Guide** The 2nd-generation Ruijie supplicant deployment function redirects the browser to a specified resource website so that the supplicant software can be downloaded. Redirection parameters need to be configured.

**Configuration Examples** The following example enables the 2nd-generation Ruijie supplicant deployment function.

```
Hostname(config)# dot1x redirect
```

**Prompt** N/A

**Platform**  
**Description**

N/A

## 1.25 dot1x reauth-max

Use this command to set the maximum re-auth attempts.

Use the **no** form of this command to restore the default setting.

**dot1x reauth-max** *num*

**no dot1x reauth-max**

| Parameter          | Parameter  | Description                                          |
|--------------------|------------|------------------------------------------------------|
| <b>Description</b> | <i>num</i> | Maximum re-auth attempts. The range is from 1 to 10. |

**Defaults** The default is 6.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Use this command to specify the maximum number of supplicant re-authentications. Use the **show dot1x** command to display 802.1X configuration.

**Configuration** The following example sets the maximum re-auth attempts to 2.

**Examples**

```
Hostname(config)# dot1x reauth-max 2
```

| Related         | Command           | Description                      |
|-----------------|-------------------|----------------------------------|
| <b>Commands</b> | <b>show dot1x</b> | Displays the 802.1X information. |

**Platform**  
**Description**

N/A

## 1.26 dot1x re-authentication

Use this command to enable timed re-authentication function.

Use the **no** form of the command to restore the default setting.

**dot1x re-authentication**

**no dot1x re-authentication**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** This function is disabled by default.



**Command** Global configuration mode  
**Mode**

**Usage Guide** This command will re-authenticate the supplicant periodically after he passes the authentication. Use the **show dot1x** command to display 802.1X configuration. The default setting is recommended.

**Configuration** The following example enables timed re-authentication function.

**Examples**

```
Hostname(config)# dot1x re-authentication
```

| Related         | Command           | Description                      |
|-----------------|-------------------|----------------------------------|
| <b>Commands</b> | <b>show dot1x</b> | Displays the 802.1X information. |

**Platform** N/A  
**Description**

## 1.27 dot1x timeout re-authperiod

Use this command to set the re-authentication interval when re-authentication is enabled.

**dot1x timeout re-authperiod** *time*

| Parameter          | Parameter   | Description                                                        |
|--------------------|-------------|--------------------------------------------------------------------|
| <b>Description</b> | <i>time</i> | Authentication interval in seconds, in the range from 1 to 65,535. |

**Defaults** The default is 3,600 seconds.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Use the **show dot1x** command to display the 802.1X configuration.

**Configuration** The following example sets the re-authentication interval to 2,400 seconds.

**Examples**

```
Hostname(config)# dot1x timeout re-authperiod 2400
```

| Related         | Command           | Description                            |
|-----------------|-------------------|----------------------------------------|
| <b>Commands</b> | <b>show dot1x</b> | Displays the information about 802.1X. |

**Platform** N/A  
**Description**

## 1.28 dot1x timeout quiet-period

Use this command to set the quiet period after authentication failure.

Use the **no** form of this command to restore the default setting.

**dot1x timeout quiet-period** *time*

| Parameter   | Parameter   | Description                                                                                   |
|-------------|-------------|-----------------------------------------------------------------------------------------------|
| Description | <i>time</i> | Sets the quiet period after authentication failure in seconds, in the range from 0 to 65,535. |

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode

**Usage Guide** When authentication fails, the supplicant must wait for a period of time before re-authentication.

**Configuration Examples** The following example sets the quiet period after authentication failure to 60 seconds.

```
Hostname(config)# dot1x timeout quiet-period 60
```

| Related  | Command           | Description                      |
|----------|-------------------|----------------------------------|
| Commands | <b>show dot1x</b> | Displays the 802.1X information. |

**Platform** N/A

**Description**

## 1.29 dot1x timeout supp-timeout

Use this command to set the authentication timeout between the device and the supplicant.

Use the **no** form of this command to restore the default setting.

**dot1x timeout supp-timeout** *time*

| Parameter   | Parameter   | Description                                                                                            |
|-------------|-------------|--------------------------------------------------------------------------------------------------------|
| Description | <i>time</i> | Authentication timeout between the device and the supplicant<br>The range is from 1 to 65,535 seconds. |

**Defaults** The default is 3 seconds.

**Command Mode** Global configuration mode

**Usage Guide** Use the **show dot1x** command to show display 802.1X configuration.

**Configuration Examples** The following example sets the authentication timeout between the device and the supplicant to 10s:

```
Hostname(config)# dot1x timeout supp-timeout 10
```

| Related Commands | Command           | Description                            |
|------------------|-------------------|----------------------------------------|
|                  | <b>show dot1x</b> | Displays the information about 802.1x. |

**Platform** N/A  
**Description**

### 1.30 dot1x timeout server-timeout

Use this command to set the server timeout interval.

**dot1x timeout server-timeout** *time*

| Parameter          | Parameter   | Description                                                            |
|--------------------|-------------|------------------------------------------------------------------------|
| <b>Description</b> | <i>time</i> | The server timeout interval in seconds, in the range from 1 to 65,535. |

**Defaults** The default is 5 seconds.

**Command Mode** Global configuration mode

**Usage Guide** By default, the timeout of the 802.1X server is less than that of the RADIUS server. Use this command to raise the 802.1X timeout so as to exceed the RADIUS value. For details, see *Configuration Guide*.

**Configuration Examples** The following example set the server timeout interval to 10 seconds.

```
Hostname(config)# dot1x timeout server-timeout 10
```

| Related Commands | Command           | Description                      |
|------------------|-------------------|----------------------------------|
|                  | <b>show dot1x</b> | Displays the 802.1X information. |

**Platform** N/A  
**Description**

### 1.31 dot1x timeout tx-period

Use this command to set the request/id packet re-transmission interval.

**dot1x timeout tx-period** *time*

| Parameter          | Parameter   | Description                                                                               |
|--------------------|-------------|-------------------------------------------------------------------------------------------|
| <b>Description</b> | <i>time</i> | The request/id packet re-transmission interval in seconds, in the range from 1 to 65,535. |

**Defaults** The default is 4 seconds.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Use the **show dot1x** command to display 802.1X configuration.

**Configuration** The following example sets the request/id packet re-transmission interval to 5 seconds.

**Examples**

```
Hostname(config)# dot1x timeout tx-period 5
```

| Related         | Command           | Description                            |
|-----------------|-------------------|----------------------------------------|
| <b>Commands</b> | <b>show dot1x</b> | Displays the information about 802.1X. |

**Platform** N/A  
**Description**

## 1.32 dot1x user-trap enable

Use this command to enable users to send online/offline traps.

Use the **no** form of this command to restore the default setting.

**dot1x user-trap enable**

**no dot1x user-trap enable**

| Parameter          | Parameter | Description                                                                                            |
|--------------------|-----------|--------------------------------------------------------------------------------------------------------|
| <b>Description</b> | N/A       | Authentication timeout between the device and the supplicant<br>The range is from 0 to 65,535 seconds. |

**Defaults** This function is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Use this command to enable users to send online/offline traps to the SNMP server.

**Configuration** The following example enables STAs to send online/offline traps.

**Examples**

```
Hostname(config)# dot1x user-trap enable
```

**Platform** N/A  
**Description**

## 1.33 dot1x valid-ip-acct enable

Use this command to enable IP address-triggered accounting.

Use the **no** form of this command to restore the default setting.

**dot1x valid-ip-acct enable**  
**no dot1x valid-ip-acct enable**

|             | Parameter | Description |
|-------------|-----------|-------------|
| Parameter   |           |             |
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable accounting only when users obtain valid IP addresses.

**Configuration** The following example enables IP address-triggered accounting.

**Examples**

```
Hostname(config)#dot1x valid-ip-acct enable
```

**Platform** N/A

**Description**

## 1.34 dot1x valid-ip-acct timeout

Use this command to configure IP address-triggered accounting timeout.

Use the **no** form of this command to restore the default setting.

**dot1x valid-ip-acct timeout *time***  
**no dot1x valid-ip-acct timeout**

|             | Parameter   | Description                                                                                               |
|-------------|-------------|-----------------------------------------------------------------------------------------------------------|
| Parameter   |             |                                                                                                           |
| Description | <i>time</i> | IP address-triggered accounting timeout in the unit of minutes.<br>The range is from 1 to 65,535 seconds. |

**Defaults** The default is 5 minutes.

**Command Mode** Global configuration mode

**Usage Guide** The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.

**Configuration** The following example configures IP address-triggered accounting timeout.

**Examples**

```
Hostname(config)# dot1x valid-ip-acct timeout 10
```

**Platform** N/A

**Description**

## 1.35 dot1x-mab

Use this command to enable MAB function in WLAN.

Use the **no** form of this command to restore the default setting.

**dot1x-mab**

**no dot1x-mab**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** (Optional) Use this command to enable MAB function for MAC-based security authentication in WLAN.

**Configuration Examples** The following example enables MAB function in WLAN.

```
Hostname(config-wlansec)# dot1x-mab
```

**Platform Description** This command is supported only on wireless products.

## 1.36 encapsulation

Use this command to configure 802.1Q encapsulation on an interface or sub-interface. Use the **no** or **default** form of this command to restore the default setting.

**encapsulation dot1q** { *vlan-id* | **group** *vlan-group-id* }

**no encapsulation**

**default encapsulation**

| Parameter Description | Parameter                               | Description                                                |
|-----------------------|-----------------------------------------|------------------------------------------------------------|
|                       | <b>dot1q</b> <i>vlan-id</i>             | Specifies a VLAN ID. The value ranges from 1 to 4094.      |
|                       | <b>dot1q group</b> <i>vlan-group-id</i> | Specifies a VLAN group ID. The value ranges from 1 to 128. |

**Defaults** 802.1Q encapsulation is not configured on an interface or sub-interface by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** Run the **encapsulation dot1q** *vlan-id* command to configure an 802.1Q encapsulation VLAN ID.  
Run the **encapsulation dot1q group** *vlan-group-id* command to configure an 802.1Q encapsulation VLAN group ID.

**Configuration Examples** The following example configures 802.1Q encapsulation VLAN group 1 on interface Dot11radio 1/0.1 on an AP.

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0.1
Hostname(config-subif)# encapsulation dot1Q group 1
    
```

**Verification** N/A

**Prompt** N/A

**Common Errors** N/A

**Platform Description** This command is supported on APs only.

### 1.37 show dot1x

Use this command to display the 802.1X setting.

**show dot1x**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command**

**Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the 802.1X setting.

```

Hostname#show dot1x

802.1X basic information:
 802.1X Status ..... enable
 Authentication Mode ..... eap
 Authorization mode ..... disable
    
```

```
Total User Number ..... 0 (exclude dynamic user)
Authenticated User Number ..... 0 (exclude dynamic user)
Dynamic User Number ..... 0
Re-authentication ..... disable
Re-authentication Period ..... 3600 seconds
Re-authentication max ..... 3 times
Quiet Period ..... 10 seconds
Tx Period ..... 30 seconds
Supplicant Timeout ..... 3 seconds
Server Timeout ..... 5 seconds
Maximum Request ..... 3 times
Client Online Probe ..... disable
Eapol Tag ..... enable
802.1x redirect ..... disable
Private supplicant only ..... disable
```

**Related  
Commands**

| Command                             | Description                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------|
| <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
| <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
| <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
| <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
| <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
| <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
| <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
| <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
| <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
| <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform** N/A

**Description**

### 1.38 show dot1x auth-address-table

Use this command to display 802.1X authentication address table.

**show dot1x auth-address-table** [ **address** *addr* | **interface** *interface* ]

**Parameter  
Description**

| Parameter        | Description                                   |
|------------------|-----------------------------------------------|
| <i>addr</i>      | Physical IP address that can be authenticated |
| <i>interface</i> | Interface number                              |



**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the 802.1X authentication address table.

**Examples**

```

Hostname# show dot1x auth-address-table
Interface      Address
-----
Gi0/1          00d0.f800.0c0e
Gi0/2          001a.c800.0102

Hostname#show dot1x auth-address-table interface fastEthernet 0/1
Interface      Address
-----
Gi0/1          00d0.f800.0c0e

Hostname#show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface      Address
-----
Gi0/1          00d0.f800.0c0e

```

**Related**

**Commands**

| Command                             | Description                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------|
| <b>dot1x auth-mode</b>              | Sets the 802.1x authentication mode.                                          |
| <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
| <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
| <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
| <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
| <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
| <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
| <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
| <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
| <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform** N/A

**Description**

## 1.39 show dot1x auto-req

Use this command to display the auto-request authentication information.

**show dot1x auto-req**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the auto-request authentication information.

### Examples

```

Hostname# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num : 0
Req-Interval: 30 Seconds

```

| Related Commands | Command                             | Description                                                                   |
|------------------|-------------------------------------|-------------------------------------------------------------------------------|
|                  | <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
|                  | <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
|                  | <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
|                  | <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
|                  | <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
|                  | <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
|                  | <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
|                  | <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
|                  | <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
|                  | <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform Description** N/A

## 1.40 show dot1x max-req

Use this command to display the maximum number of request/challenge packet transmission.

**show dot1x max-req**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the maximum number of request/challenge packet transmission.

```
Hostname#show dot1x max-req
```

```
Max-Req: 3 Times
```

| Related Commands | Command                             | Description                                                                   |
|------------------|-------------------------------------|-------------------------------------------------------------------------------|
|                  | <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
|                  | <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
|                  | <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
|                  | <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
|                  | <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
|                  | <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
|                  | <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
|                  | <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
|                  | <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
|                  | <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform** N/A

**Description**

## 1.41 show dot1x port-control

Use this command to display the port-control information.

**show dot1x port-control [ interface interface-type interface-number]**

| Parameter   | Parameter               | Description    |
|-------------|-------------------------|----------------|
| Description | <i>interface-type</i>   | Interface type |
|             | <i>interface-number</i> | Interface ID   |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the port-control information.

**Examples**

```

Hostname# show dot1x port-control
Interface Mode          Dynamic-User Static-User Max-User Authened MAB
-----
Gi0/5   mac-based 0          0          unlimited no      disable

```

| Related Commands | Command                             | Description                                                                   |
|------------------|-------------------------------------|-------------------------------------------------------------------------------|
|                  | <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
|                  | <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
|                  | <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
|                  | <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
|                  | <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
|                  | <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
|                  | <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
|                  | <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
|                  | <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
|                  | <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform** N/A

**Description**

## 1.42 show dot1x private-supplicant-only

Use this command to display the information about the private supplicant.

**show dot1x private-supplicant-only**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |     |     |
|--------------------|-----|-----|
| <b>Description</b> | N/A | N/A |
|--------------------|-----|-----|

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the information about the private supplicant:

**Examples**

```

Hostname# show dot1x private-supPLICANT-only

private-supPLICANT-only: Disabled

```

**Related Commands**

| Command                             | Description                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------|
| <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
| <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
| <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
| <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
| <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
| <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
| <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
| <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
| <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
| <b>dot1x timeout tx-period</b>      | Sets the re-transmission interval.                                            |

**Platform** N/A

**Description**

## 1.43 show dot1x probe-timer

Use this command to display the configuration of online user probe.

**show dot1x probe-timer**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration of online user probe.

```

Examples
Hostname# show dot1x probe-timer
Hello Interval      : 20
Hello Alive        : 60
    
```

Field Description

| Command        | Description                    |
|----------------|--------------------------------|
| Hello Interval | Sets the probe period.         |
| Hello Alive    | Sets the probe alive interval. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A.        |

**Platform** N/A

**Description**

### 1.44 show dot1x re-authentication

Use this command to display re-authentication status.

**show dot1x re-authentication**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example displays re-authentication status.

```

Examples
Hostname# show dot1x re-authentication

Reauth-Enabled: Disabled
    
```

| Command        | Description                          |
|----------------|--------------------------------------|
| Reauth-Enabled | Whether to enable re-authentication. |

| Related | Command | Description |
|---------|---------|-------------|
|---------|---------|-------------|

|                 |     |     |
|-----------------|-----|-----|
| <b>Commands</b> | N/A | N/A |
|-----------------|-----|-----|

**Platform** N/A

**Description**

## 1.45 show dot1x reauth-max

Use this command to display the maximum re-auth attempts.

**show dot1x reauth-max**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the maximum re-authentication attempts.

```
Hostname# show dot1x reauth-max
```

```
Reauth-Max: 3 Times
```

| Command        | Description                                  |
|----------------|----------------------------------------------|
| Reauth-Enabled | Sets the maximum re-authentication attempts. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.46 show dot1x summary

Use this command to display the 802.1X authentication summary.

**show dot1x summary**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode/Global configuration mode/Interface configuration mode  
**Mode**

**Usage Guide** It is convenient to display the 802.1X authentication summary according to the MAC address or username.

**Configuration** The following example displays the summary of 802.1X authentication.

```

Examples
Hostname# show dot1x summary
ID      User      MAC          Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time
-----
-----
    
```

| <b>Related Commands</b>        | <b>Command</b>                      | <b>Description</b>                                                            |
|--------------------------------|-------------------------------------|-------------------------------------------------------------------------------|
|                                | <b>dot1x auth-mode</b>              | Sets the 802.1X authentication mode.                                          |
|                                | <b>dot1x max-req</b>                | Sets the maximum number of authentication request re-transmissions.           |
|                                | <b>dot1x port-control auto</b>      | Sets the port to participate in authentication.                               |
|                                | <b>dot1x reauth-max</b>             | Sets the maximum number of the supplicant re-authentications.                 |
|                                | <b>dot1x re-authentication</b>      | Sets the re-authentication attribute.                                         |
|                                | <b>dot1x timeout quiet-period</b>   | Sets the time the device waits before re-authentication.                      |
|                                | <b>dot1x timeout re-authperiod</b>  | Sets the re-authentication period for the supplicant.                         |
|                                | <b>dot1x timeout server-timeout</b> | Sets the authentication timeout between the device and authentication server. |
|                                | <b>dot1x timeout supp-timeout</b>   | Sets the authentication timeout between the device and the supplicant.        |
| <b>dot1x timeout tx-period</b> | Sets the re-transmission interval.  |                                                                               |

**Platform** N/A

**Description**

### 1.47 show dot1x timeout quiet-period

Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

**show dot1x timeout quiet-period**

| <b>Parameter</b>   | <b>Parameter</b> | <b>Description</b> |
|--------------------|------------------|--------------------|
| <b>Description</b> | N/A              | N/A                |



**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.

**Configuration Examples** The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.

```
Hostname#show dot1x timeout quiet-period
```

```
Quiet-Period: 10 Seconds
```

Parameter Description:

| Parameter    | Description                                                                                |
|--------------|--------------------------------------------------------------------------------------------|
| Quiet-Period | The time for the device to wait before re-authentication after the authentication failure. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

### 1.48 show dot1x timeout re-authperiod

Use this command to display the re-authentication interval.

**show dot1x timeout re-authperiod**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the re-authentication interval.

**Configuration Examples** The following example displays the re-authentication interval.:

```
Hostname#show dot1x timeout re-authperiod
```

```
Reauth-Period: 3600 Seconds
```

Parameter Description:

| Parameter     | Description                 |
|---------------|-----------------------------|
| Reauth-Period | Re-authentication interval. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform  
Description

N/A

## 1.49 show dot1x timeout server-timeout

Use this command to display the authentication timeout period.

**show dot1x timeout server-timeout**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

Defaults

N/A

Command Mode  
Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide  
Use this command to display the authentication timeout period.

Configuration  
Use this command to display the authentication timeout period:

Examples  
Hostname#show dot1x timeout server-timeout

```
Server-Timeout: 5 Seconds
```

Parameter Description:

| Parameter     | Description                                  |
|---------------|----------------------------------------------|
| Server-Period | AuthenticationServer timeout periodinterval. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform  
Description

N/A

## 1.50 show dot1x timeout supp-timeout

Use this command to display the request/challenge packets re-transmission interval.

**show dot1x timeout supp-timeout**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the request/challenge packets re-transmission interval.

**Configuration** Use this command to display the request/challenge packets re-transmission interval:

**Examples**

```

Hostname# show dot1x timeout supp-timeout

Supp-Timeout: 3 Seconds
    
```

Field Description:

| Field         | Description                                             |
|---------------|---------------------------------------------------------|
| Server-Period | The request/challenge packets re-transmission interval. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.51 show dot1x timeout tx-period

Use this command to display the request/id packets re-transmission interval.

**show dot1x timeout tx-period**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use this command to display the request/id packets re-transmission interval.

**Configuration** Use this command to display the request/ id packets re-transmission interval:

**Examples**

```

Hostname# show dot1x timeout tx-period
    
```

Tx-Period: 30 Seconds

Parameter Description:

| Parameter | Description                                  |
|-----------|----------------------------------------------|
| Tx-Period | Request/id packets re-transmission interval. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A

Description

## 1.52 show dot1x user mac

Use this command to display the information about 802.1X authentication users based on MAC addresses.

**show dot1x user mac** *mac-addr*

| Parameter   | Parameter       | Description |
|-------------|-----------------|-------------|
| Description | <i>mac-addr</i> | MAC address |

Defaults N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.

**Configuration Examples** The following example displays the information about the 802.1X authentication user according to the user's MAC address.

```

Hostname#show dot1x user mac 0023.aaaa.4286

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aaaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds

```

```

Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :

```

Parameter Description:

| Parameter                    | Description                             |
|------------------------------|-----------------------------------------|
| User name                    | User name                               |
| User id                      | User ID mode                            |
| Type                         | User type                               |
| Mac address                  | User's MAC address                      |
| Vlan id                      | User VLAN ID                            |
| Access from port             | The port that user access from          |
| Time online                  | User online time                        |
| User ip address              | User IP address                         |
| Max user number on this port | The maximum number of users on the port |
| Authorization session time   | The authorized session time             |
| Supplicant is private        | Whether the terminal is a Ruijie device |
| Start accounting             | The accounting is enabled.              |
| Permit proxy user            | The user is allowed to use the proxy.   |
| Permit dial user             | The user is allowed to dial.            |
| IP privilege                 | The IP privilege level                  |
| user acl-name                | The ACL information                     |

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

Platform N/A

Description

## 1.53 show dot1x user name

Use this command to display information about 802.1X authentication users based on usernames.

**show dot1x user name** *name*

| Parameter   | Parameter   | Description |
|-------------|-------------|-------------|
| Description | <i>name</i> | User name   |

Defaults N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** Use the **show dot1x summary** command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.

**Configuration** The following example displays the information about the 802.1X authentication user according to the user name.

**Examples**

```

Hostname#show dot1x user name ts-user

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Inner-VLAN id 5 Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :

```

Parameter Description:

| Parameter                    | Description                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User name                    | User name                                                                                                                                                                           |
| User id                      | User ID mode                                                                                                                                                                        |
| Type                         | User type                                                                                                                                                                           |
| Mac address                  | User's MAC address                                                                                                                                                                  |
| Vlan id                      | User VLAN ID                                                                                                                                                                        |
| Inner-VLAN id                | ID of the inner VLAN, to which the client participating in authentication belongs. The device that supports dual tags of users participating in authentication supports this field. |
| Access from port             | The port that user access from                                                                                                                                                      |
| Time online                  | User online time                                                                                                                                                                    |
| User ip address              | User IP address                                                                                                                                                                     |
| Max user number on this port | The maximum number of users on the port                                                                                                                                             |
| Authorization session time   | The authorized session time                                                                                                                                                         |
| Supplicant is private        | Whether the terminal is a Ruijie device.                                                                                                                                            |
| Start accounting             | The accounting is enabled.                                                                                                                                                          |
| Permit proxy user            | The user is allowed to use the proxy.                                                                                                                                               |

|                  |                              |
|------------------|------------------------------|
| Permit dial user | The user is allowed to dial. |
| IP privilege     | The IP privilege level.      |
| user acl-name    | The ACL information.         |

|                             |                |                    |
|-----------------------------|----------------|--------------------|
| <b>Related<br/>Commands</b> | <b>Command</b> | <b>Description</b> |
|                             | N/A            | N/A                |

**Platform** N/A

**Description**

## 1.54 show vlan-group

Use this command to display VLAN group information on an AP.

**show vlan-group** [ *vlan-group-id* ]

| Parameter Description | Parameter            | Description                                                |
|-----------------------|----------------------|------------------------------------------------------------|
|                       | <i>vlan-group-id</i> | Specifies a VLAN group ID. The value ranges from 1 to 128. |

**Command** All modes except the user EXEC mode

**Mode**

**Default Level** 2

**Usage Guide** -

**Configuration** The following example displays VLAN members of all VLAN groups.

**Examples**

```

Hostname# show vlan-group
vlan-group id      mode      default-vlan  vlan-list
-----
1                 dot1x    0
10                dot1x    10            10-15
11                dot1x    0
  
```

**Prompt** N/A

**Platform Description** N/A

## 1.55 vlan-assign-mode

Use this command to configure the VLAN configuration delivery mode for a VLAN group. Use the no form of this command to restore the default setting.

**vlan-assign-mode dot1x**

**no vlan-assign-mode**

| Parameter Description | Parameter    | Description                                                                                 |
|-----------------------|--------------|---------------------------------------------------------------------------------------------|
|                       | <b>dot1x</b> | The authentication server delivers VLAN configuration after 802.1X authentication succeeds. |



|                               |                                                                                                                                                                                                        |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>               | No VLAN configuration delivery mode is configured for a VLAN group.                                                                                                                                    |
| <b>Command Mode</b>           | VLAN group configuration mode and global configuration mode                                                                                                                                            |
| <b>Default Level</b>          | 14                                                                                                                                                                                                     |
| <b>Usage Guide</b>            | Global configuration applies to all VLAN groups.<br>VLAN group-based configuration applies to only the current VLAN group.<br>VLAN group-based configuration take priority over global configuration.  |
| <b>Configuration Examples</b> | The following example sets the VLAN configuration delivery mode to <b>dot1x</b> for VLAN group 10.<br><pre> Hostname(config)# vlan-group 10 Hostname(config-vlan-group)# vlan-assign-mode dot1x </pre> |
| <b>Verification</b>           | Run the <b>show vlan-group 10</b> to check the VLAN configuration delivery mode for VLAN group 10.                                                                                                     |
| <b>Prompt</b>                 | N/A                                                                                                                                                                                                    |
| <b>Common Errors</b>          | N/A                                                                                                                                                                                                    |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                    |

## 1.56 vlan-group(Global configuration mode)

Use this command to create a VLAN group. Use the **no** form of this command to remove the configuration.

**vlan-group** *vlan-group-id*

**no vlan-group** *vlan-group-id*

| Parameter Description | Parameter            | Description                                                |
|-----------------------|----------------------|------------------------------------------------------------|
|                       | <i>vlan-group-id</i> | Specifies a VLAN group ID. The value ranges from 1 to 128. |

|                      |                           |
|----------------------|---------------------------|
| <b>Defaults</b>      | -                         |
| <b>Command Mode</b>  | Global configuration mode |
| <b>Default Level</b> | 14                        |

**Usage Guide** N/A

**Configuration** The following example creates VLAN group 100 on an AP.

**Examples**

```

Hostname# configure terminal
Hostname(config)# vlan-group 100

```

**Verification** Run the **show vlan-group 100** to check VLAN group 100 configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.57 vlan-group(WLAN configuration mode)

Use this command to associate the WLAN with a VLAN group.

**vlan-group** *vlan-group-id*

| Parameter Description | Parameter            | Description                                             |
|-----------------------|----------------------|---------------------------------------------------------|
|                       | <i>vlan-group-id</i> | Specifies a VLAN group. The value ranges from 1 to 128. |

**Defaults** The WLAN is associated with no VLAN group by default.

**Command Mode** WLAN configuration mode

**Default Level** 14

**Usage Guide** -

**Configuration** The following example associates WLAN 1 with VLAN group 100 on an AP.

**Examples**

```

Hostname# configure terminal
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# vlan-group 100

```

**Verification** -

**Prompt** N/A

**Common Errors** N/A

**Platform Description** This command is supported on APs only.

## 1.58 vlan-list

Use this command to configure VLAN members for a VLAN group. Use the no form of this command to restore the default setting.

**vlan-list**   *vlan-list*

**no**   *vlan-list*

| Parameter Description | Parameter          | Description                                                                   |
|-----------------------|--------------------|-------------------------------------------------------------------------------|
|                       | <i> vlan-list </i> | Configures VLAN members for a VLAN group. Up to 128 VLAN members are allowed. |

**Defaults** A VLAN group contains no members by default.

**Command Mode** VLAN group configuration mode

**Default Level** 14

**Usage Guide** If a WLAN needs to be mapped to multiple VLANs, add these VLANs to a VLAN group and associate the VLAN group with the WLAN.

**Configuration Examples** The following example adds VLANs 100-105 to VLAN group 100 on an AP.

```

Hostname# configure terminal
Hostname(config)# vlan-group 100
Hostname(config-vlan-group)# vlan-list 100-105

```

**Verification** Run the **show vlan-group 100** to check VLAN member configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

# 1 Authentication

## 1.1 accounting

Use this command to set an accounting method for the template.

Use the **no** form of this command to restore the default setting.

**accounting** { *method-list* }

**no accounting**

| Parameter Description | Parameter          | Description             |
|-----------------------|--------------------|-------------------------|
|                       | <i>method-list</i> | Name of the method list |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** The *method-list* parameter in this command should be consistent with network accounting list name configured in AAA.

**Configuration Examples** The following example sets the **mlist1** accounting method for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)# accounting mlist1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 authentication

Use this command to set an authentication method for the template.

Use the **no** form of this command to restore the default setting.

**authentication** { *method-list* }

**no authentication**

| Parameter Description | Parameter          | Description             |
|-----------------------|--------------------|-------------------------|
|                       | <i>method-list</i> | Name of the method list |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** The *method-list* parameter in this command should be consistent with the Web authentication method list configured in AAA.  
The first generation authentication does not support the authentication method list configuration.

**Configuration Examples** The following example sets the **mlist1** authentication method for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)#authentication mlist1
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.3 bindmode

Use this command to set a binding mode for the template.

Use the **no** form of this command to restore the default setting.

**bindmode ip-mac-mode**

**no bindmode**

**Parameter Description**

| Parameter          | Description                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>ip-mac-mode</b> | Enable IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry. |

**Defaults** N/A

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example adopts the IP only mode for the **eportalv2** template.

```
Hostname(config.tmplt.eportalv2)# bindmode ip-mac-mode
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.4 clear web-auth acl

Use this command to clear all blacklists and whitelists.

**clear web-auth acl [ black-ip | black-port | black-url | white-port | white-url ]**

| Parameter Description | Parameter         | Description                     |
|-----------------------|-------------------|---------------------------------|
|                       |                   | <b>white-url</b>                |
|                       | <b>white-port</b> | Clears ports in all whitelists. |
|                       | <b>black-url</b>  | Clears URLs in all blacklists.  |
|                       | <b>black-ip</b>   | Clears IPs in all blacklists.   |
|                       | <b>black-port</b> | Clears ports in all blacklists. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears all blacklists and whitelists.

```
Hostname# clear web-auth acl
```

**Platform Description** N/A

## 1.5 clear web-auth direct-arp

Use this command to clear all Address Resolution Protocol (ARP) resources

**clear web-auth direct-arp**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration** The following example clears all ARP resources.

**Examples** `Hostname# clear web-auth direct-arp`

**Prompt** N/A

**Platform Description** N/A

## 1.6 clear web-auth direct host

Use this command to clear all authentication-exempted users.

**clear web-auth direct-host**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example clears all authentication-exempted users.

**Examples** `Hostname# clear web-auth direct-host`

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.7 clear web-auth direct-site

Use this command to clear all authentication-exempted network resources.

**clear web-auth direct-site**

**Parameter**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                         |                                                                             |                    |
|-------------------------|-----------------------------------------------------------------------------|--------------------|
| <b>Description</b>      |                                                                             |                    |
|                         | N/A                                                                         | N/A                |
| <b>Defaults</b>         | N/A                                                                         |                    |
| <b>Command Mode</b>     | Privileged EXEC mode                                                        |                    |
| <b>Usage Guide</b>      | N/A                                                                         |                    |
| <b>Configuration</b>    | The following example clears all authentication-exempted network resources. |                    |
| <b>Examples</b>         | <pre>Hostname# clear web-auth direct-site</pre>                             |                    |
| <b>Related Commands</b> |                                                                             |                    |
|                         | <b>Command</b>                                                              | <b>Description</b> |
|                         | N/A                                                                         | N/A                |
| <b>Platform</b>         | N/A                                                                         |                    |
| <b>Description</b>      |                                                                             |                    |

## 1.8 clear web-auth user

Use this command to force the user to go offline.

**clear web-auth user** { **all** | **ip** *ip-address* | **ip** *ipv6-address* | **mac** *mac-address* | **name** *name-string* }

|                              |                                                       |                                    |
|------------------------------|-------------------------------------------------------|------------------------------------|
| <b>Parameter Description</b> | <b>Parameter</b>                                      | <b>Description</b>                 |
|                              | <i>ip-address</i>                                     | Specifies the user's IPv4 address. |
|                              | <i>ipv6-address</i>                                   | Specifies the user's IPv6 address. |
|                              | <i>mac-address</i>                                    | Specifies the user's MAC address.  |
|                              | <i>name-string</i>                                    | Specifies the user name.           |
| <b>Defaults</b>              | N/A                                                   |                                    |
| <b>Command Mode</b>          | Privileged EXEC mode                                  |                                    |
| <b>Usage Guide</b>           | N/A                                                   |                                    |
| <b>Configuration</b>         | The following example forces all users to go offline. |                                    |
| <b>Examples</b>              | <pre>Hostname(config) clear web-auth user all</pre>   |                                    |
| <b>Related</b>               | <b>Command</b>                                        | <b>Description</b>                 |



|                 |     |     |
|-----------------|-----|-----|
| <b>Commands</b> |     |     |
|                 | N/A | N/A |

**Platform** N/A

**Description**

## 1.9 domain

Use this command to enable automatic adding of domain information after usernames.

**domain** *domain-string*

| Parameter          | Parameter            | Description                                                   |
|--------------------|----------------------|---------------------------------------------------------------|
| <b>Description</b> | <i>domain-string</i> | Domain information to be automatically added after usernames. |

**Command** Template configuration mode.

**Mode**

**Default Level** 14

**Usage Guide** N/A

**Configuration** The following example configures automatic adding of domain information "@wifi" after usernames:

**Examples**

```
Hostname(config. tmplt. eportalv2)#domain @wifi
```

**Prompt** N/A

**Platform** N/A

**Description**

## 1.10 fmt

Use this command to set the URL redirection format in the second template configuration mode.

**fmt** { **cmcc-ext1** | **cmcc-ext2** | **cmcc-mtx** | **cmcc-normal** | **cmcc-ext3** | **ct-jc** | **cucc** | **custom** | **default** }

URL format defined for the first-generation web authentication template:

**fmt** { **ace** | **default** | **custom** }

Use this command to set the custom URL redirection format in the first & second template configuration modes.

**fmt custom** [ **encyr** { **md5** | **des** | **des\_ecb** | **des\_ecb3** | **none** } ] [ **user-ip** *userip-str* ] [ **user-mac** *usermac-str* ] [ **mac-format** { **dot** | **line** | **none** | **5colon** } ] [ **user-vid** *uservid-str* ] [ **user-id** *userid-str* ] [ **nas-ip** *nasip-str* ] [ **nas-id** *nasid-str* ] [ **nas-id2** *nasid2-str* ] [ **ac-name** *acname-str* ] [ **ac-name** *acname-str* ] [ **ap-mac** *apmac-str* ] [ **mac-format** { **dot** | **line** | **none** | **5colon** } ] [ **url** *url-str* ] [ **ssid**

*ssid-str* ] [ **port** *port-str* ] [ **ac-serialno** *ac-sno-str* ] [ **ap-serialno** *ap-sno-str* ] [ **ap-name** *apname-str* ] [ **ap-group** *apgroup-str* ] [ **additional** *extern-str* ]

Use the **no** form of **fmt custom** command to remove the custom URL redirection format.

**no** **fmt custom** [ **user-ip** ] [ **user-mac** ] [ **user-vid** ] [ **user-id** ] [ **nas-ip** ] [ **nas-id** ] [ **nas-id2** ] [ **ac-name** ] [ **ap-mac** ] [ **url** ] [ **ssid** ] [ **port** ] [ **ac-serialno** ] [ **ap-serialno** ] [ **ap-name** ] [ **ap-group** ] [ **additional** ]

**Parameter  
Description**

| Parameter          | Description                                 |
|--------------------|---------------------------------------------|
| <b>cmcc-ext1</b>   | Extended CMCC format                        |
| <b>cmcc-ext2</b>   | Liaoning CMCC format                        |
| <b>cmcc-ext3</b>   | Ningbo/Jiaxing format for AC manufacturers  |
| <b>cmcc-mtx</b>    | CMCC format for AC manufacturers            |
| <b>cmcc-normal</b> | Standard CMCC format                        |
| <b>ct-jc</b>       | China Telecom format                        |
| <b>cucc</b>        | Shandong China Unicom format                |
| <b>ace</b>         | Supports ACE correlation.                   |
| <b>default</b>     | Ruijie format                               |
| <b>custom</b>      | Custom format                               |
| <i>userip-str</i>  | User IP address string                      |
| <i>usermac-str</i> | User MAC address string                     |
| <i>userid-str</i>  | User VID string                             |
| <i>nasip-str</i>   | NAS device IP address string                |
| <i>nasid-str</i>   | NAS device ID string                        |
| <i>nasid2-str</i>  | NAS device ID string (supports 2 NAS ID)    |
| <i>acname-str</i>  | AC name string                              |
| <i>apmac-str</i>   | Associated AP MAC address string            |
| <i>url-str</i>     | Original URL string                         |
| <i>ssid-str</i>    | SSID string                                 |
| <i>port-str</i>    | Auth-Port string                            |
| <i>ac-sno-str</i>  | Serial number string of the AC              |
| <i>ap-sno-str</i>  | Serial number string of the AP              |
| <i>apname-str</i>  | AP name                                     |
| <i>apgroup-str</i> | AP group name                               |
| <i>extern-str</i>  | Special strings for specific portal servers |
| <i>md5</i>         | MD5 encryption                              |
| <i>des</i>         | DES encryption                              |
| <i>des_ecb</i>     | DES_ECB encryption                          |
| <i>des_ecb3</i>    | DES_ECB3 encryption                         |
| <i>none</i>        | Not-encrypted                               |

**Defaults**

The URL redirection format is **default** in 1st and 2nd generation template configuration mode and

**clearpass** in cpweb template configuration mode.

**Command** Template configuration mode  
**Mode**

**Usage Guide** Use this command to set the URL redirection format based on the corresponding portal standard.

**Configuration** The following example sets the URL redirection format to extended CMCC format.

**Examples**

```
Hostname(config.tmplt.eportalv2)# fmt cmcc-ext1
```

**Platform** N/A  
**Description**

## 1.11 gateway-id

Use this command to set the value of **gw\_id** in the WiFiDog standard protocol used for the interaction between the devices authenticated via WiFiDog and the server.

**gateway-id** *string*

Use the **no** form of this command to delete the value of **gw\_id** from the WiFiDog standard protocol used for the interaction between the devices authenticated via WiFiDog and the server.


**no gateway-id**

| Parameter Description | Parameter     | Description                                                                                     |
|-----------------------|---------------|-------------------------------------------------------------------------------------------------|
|                       | <i>string</i> | Indicates the value of <b>gw_id</b> in the WiFiDog protocol used by the devices and the server. |

**Defaults** The value of **gw\_id** is set to the SN of the local device by default.

**Command** Template configuration mode.  
**Mode**

**Default Level** 14

**Usage Guide**  The value of **gw\_id** is set to the SN of the local device by default. Manual configuration is not required unless there is a special interworking requirement. This configuration is mandatory in hot standby and VAC scenarios, which present multiple devices as one.

**Configuration** 1. The following example sets the value of **gw\_id** in the WiFiDog protocol used by the devices and the server to **14144b6fb807**.

**Examples**

```
Hostname(config.tmplt.wifidog)#gateway-id 14144b6fb807
```

**Verification** Run the **show running-config** command to display the currently configured template parameters.

## 1.12 http redirect adapter ios

Use this command to enable automatic IOS window pop-up.

**http redirect adapter ios**

**no http redirect adapter ios**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables automatic IOS window pop-up.

```
Hostname# http redirect adapter ios
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.13 http redirect direct-arp

Use this command to set the address range of the authentication-exempted ARP.

Use the **no** form of this command to restore the default setting.

**http redirect direct-arp** { *ip-address* [ *ip-mask* ] }

**no http redirect direct-arp** { *ip-address* [ *ip-mask* ] }

| Parameter Description | Parameter         | Description          |
|-----------------------|-------------------|----------------------|
|                       | <i>ip-address</i> | IPv4 address         |
|                       | <i>ip-mask</i>    | (Optional) IPv4 mask |

**Defaults** No authentication-exempted ARP resource is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.

**Configuration** The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource.

**Examples**

```
Hostname(config)# http redirect direct-arp 172.16.0.1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.14 http redirect direct-site

Use this command to set the range of authentication-exempted network resources.

Use the **no** form of this command to restore the default setting.

**http redirect direct-site** *ipv4-address* [ *mask* ] [ **arp** | *port-number...* ]

**http redirect direct-site** *ipv6-address*

**no http redirect direct-site** *ipv4-address* [ *mask* ]

**no http redirect direct-site** *ipv6-address*

| Parameter Description | Parameter          | Description                                                                                                                                                                                               |
|-----------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                    | <i>ipv6-address</i>                                                                                                                                                                                       |
|                       | <i>ip-address</i>  | IPv4 address of the authentication-exempted network resources                                                                                                                                             |
|                       | <i>ip-mask</i>     | IPv4 address mask of the authentication-exempted network resources (optional)                                                                                                                             |
|                       | <i>port-number</i> | Port number of the transport layer. The parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.                                                                        |
|                       | <b>arp</b>         | If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only. |

**Defaults** No authentication-exempted network resource is set.

**Command** Global configuration mode

**Mode**

**Usage Guide** When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites. Up to 50 authentication-exempted users are supported.

**Configuration Examples** The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource.

```
Hostname(config)# http redirect direct-site 172.16.0.1
```

**Related Commands**

| Command                   | Description                                  |
|---------------------------|----------------------------------------------|
| <b>show http redirect</b> | Displays the HTTP redirection configuration. |

**Platform** N/A

**Description**

## 1.15 http redirect port

Use this command to redirect users' HTTP redirection request to a certain destination port.

Use the **no** form of this command to restore the default setting.

**http redirect port** *port-num*

**no http redirect port** *port-num*

**Parameter Description**

| Parameter       | Description                                                         |
|-----------------|---------------------------------------------------------------------|
| <i>port-num</i> | Destination port of the HTTP request, in the range from 1 to 65535. |

**Defaults** The default is port 80.

**Command Mode** Global configuration mode

**Usage Guide** When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page.

By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources.

This command is used to change the destination port of HTTP packets that are intercepted by the access device.

A maximum of 10 different destination port numbers can be configured, excluding default ports 80 and 443.

**Configuration** The following example redirects users' HTTP requests with port 8080.

**Examples**

```
Hostname(config)# http redirect port 8080
```

The following example does not redirect users' HTTP requests with port 80.

```
Hostname(config)# no http redirect port 80
```

**Related  
Commands**

| Command                   | Description                                  |
|---------------------------|----------------------------------------------|
| <b>show http redirect</b> | Displays the HTTP redirection configuration. |

**Platform** N/A

**Description**

## 1.16 http redirect session-limit

Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port.

Use the **no** form of this command to restore the default setting.

**http redirect session-limit** *session-num*

**no http redirect session-limit**

**Parameter  
Description**

| Parameter          | Description                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------|
| <i>session-num</i> | Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255. |

**Defaults** Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.

**Command** Global configuration mode

**Mode**

**Usage Guide** To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device.

In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1

**Configuration** The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4.

**Examples**

```
Hostname(config)# http redirect session-limit 4
```

**Related**

| Command | Description |
|---------|-------------|
|---------|-------------|

| Commands                  |                                              |
|---------------------------|----------------------------------------------|
| <b>show http redirect</b> | Displays the HTTP redirection configuration. |

**Platform** N/A

**Description**

## 1.17 http redirect timeout

Use this command to set the timeout for the redirection connection maintenance.

Use the **no** form of this command to restore the default setting.

**http redirect timeout** *seconds*

**no http redirect timeout**

| Parameter Description | Parameter      | Description                                                                                                       |
|-----------------------|----------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Set the timeout for the redirection connection maintenance. The value ranges from 1 to 10 in the unit of seconds. |

**Defaults** The default is 3 seconds.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.

**Configuration Examples** The following example sets the timeout for the redirection connection maintenance to 4 seconds.

```
Hostname(config)# http redirect timeout 4
```

| Related Commands | Command                   | Description                                  |
|------------------|---------------------------|----------------------------------------------|
|                  | <b>show http redirect</b> | Displays the HTTP redirection configuration. |

**Platform** N/A

**Description**

## 1.18 IP address

Use this command to set an IP address for the portal server.

Use the **no** form of this command to restore the default setting.

**ip** { *ip-address* | *ipv6-address* }



**no ip**

| Parameter Description | Parameter           | Description                           |
|-----------------------|---------------------|---------------------------------------|
|                       | <i>ip-address</i>   | The IPv4 address of the portal server |
|                       | <i>ipv6-address</i> | The IPv6 address of the portal server |

**Defaults** No IP address is set for the portal server by default.

**Command Mode** Template configuration mode

**Usage Guide** This command takes place of the **http redirect** [*ip-address*] command, which is now hidden as a compatible command.

**Configuration Examples** The following example sets the IP address of the eportalv1 template to 172.16.0.1.

```

Hostname(config.tmplt.eportalv1)# ip 172.16.0.1
Hostname(config.tmplt.eportalv1)#

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.19 ip portal source-interface

Use this command to specify a communication port for the portal server.

Use the **no** form of this command to restore the default setting.

**ip portal source-interface** *interface-type interface-num*

**no ip portal source-interface**

| Parameter Description | Parameter             | Description |
|-----------------------|-----------------------|-------------|
|                       | <i>interface-type</i> | Port type   |
|                       | <i>interface-num</i>  | Port No.    |

**Defaults** No communication interface is specified by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example specifies an aggregate port as the communication port.

**Examples**

```
Hostname(config)# ip portal source-interface bvi 1
```

**Platform Description** N/A

## 1.20 iportal nat enable

Use this command to enable NAT function for local Web authentication.

Use the **no** form of this command to restore the default setting.

**iportal nat enable**

**no iportal nat enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** NAT is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example enables NAT function for local Web authentication.

**Examples**

```
Hostname(config)# iportal nat enable
```

**Platform Description** N/A

## 1.21 iportal retransmit

Use this command to set the retransmission count of HTTP packets.

Use the **no** form of this command to restore the default setting.

**iportal retransmit times**

**no iportal retransmit**

| Parameter Description | Parameter    | Description                                      |
|-----------------------|--------------|--------------------------------------------------|
|                       | <i>times</i> | Retransmission count, in the range from 0 to 13. |

|                             |                                                                           |
|-----------------------------|---------------------------------------------------------------------------|
| <b>Defaults</b>             | The retransmission count of HTTP packets is 3 by default.                 |
| <b>Command Mode</b>         | Global configuration mode                                                 |
| <b>Usage Guide</b>          | N/A                                                                       |
| <b>Configuration</b>        | The following example sets the retransmission count of HTTP packets to 5. |
| <b>Examples</b>             | <pre>Hostname(config)# iportal retransmit 5</pre>                         |
| <b>Platform Description</b> | N/A                                                                       |

## 1.22 iportal service

Use this command to configure a service template.

Use the **no** form of this command to restore the default setting.

**iportal service** [ **internet** *internet-name* | **local** *local-name* ]

**no iportal service** [ **internet** *internet-name* | **local** *local-name* ]

| <b>Parameter Description</b> | Parameter            | Description           |
|------------------------------|----------------------|-----------------------|
|                              | <i>internet-name</i> | External service name |
|                              | <i>local-name</i>    | Local service name    |

|                             |                                                              |
|-----------------------------|--------------------------------------------------------------|
| <b>Defaults</b>             | No service template is configured by default.                |
| <b>Command Mode</b>         | Global configuration mode                                    |
| <b>Usage Guide</b>          | N/A                                                          |
| <b>Configuration</b>        | The following example configures a local service template.   |
| <b>Examples</b>             | <pre>Hostname(config)# iportal service local local-srv</pre> |
| <b>Platform Description</b> | N/A                                                          |

## 1.23 iportal user-agent

Use this command to configure the User Agent (UA) name. Use the **no** form of this command to remove the configuration.

**iportal user-agent** *ua-name* **type** **mobile** *ua-string*

**no iportal user-agent** *ua-name* **type mobile** *ua-string*

| Parameter Description | Parameter        | Description              |
|-----------------------|------------------|--------------------------|
|                       | <i>ua-name</i>   | Specifies the UA name.   |
|                       | <i>ua-string</i> | Specifies the UA string. |

**Defaults** No UA name is configured by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is not available now. It is replaced by client identification.

**Configuration Example** N/A

**Verification** N/A

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.24 key

Use this command to set the communication key between the Wechat access device and the authentication server.

Use the **no** form of this command to clear the communication key.

**key** *key-string*

**no key**

| Parameter Description | Parameter         | Description                                                                      |
|-----------------------|-------------------|----------------------------------------------------------------------------------|
|                       | <i>key-string</i> | Communication key between the Wechat access device and the authentication server |

**Defaults** No key is set by default.

**Command Mode** Template configuration mode

**Usage Guide** To use the Web authentication function, the communication key between the Wechat access device and the authentication server must be set as the same.

**Configuration Examples** The following example sets the communication key between the Wechat access device and the authentication server to webkey.

```
Hostname(config.tmplt.wechat)# key webkey
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.25 login-popup

Use this command to configure a pre-login popup advertisement.

Use the **no** form of this command to restore the default setting.

**login-popup** *url-string*

**no login-popup**

**Parameter Description**

| Parameter         | Description       |
|-------------------|-------------------|
| <i>url-string</i> | Advertisement URL |

**Defaults** No pre-login popup advertisement is configured by default.

**Command Mode** Template configuration mode

**Usage Guide** The URL of the popup advertisement should begin with "http://" or "https://".

**Configuration Examples** The following example configures a pre-login popup advertisement.

```
Hostname(config.tmplt.iportal)# login-popup http://www.ruijie.com.cn
```

**Platform Description** N/A

## 1.26 nas-ip

Use this command to configure the IP address of the Wechat access device.

Use the **no** form of this command to restore the default setting.

**nas-ip** { *ip-address* }

**no nas-ip**

**Parameter  
Description**

| Parameter         | Description  |
|-------------------|--------------|
| <i>ip-address</i> | IPv4 address |


**Defaults**

No IPv4 address is configure for the Wechat access device by default.

**Command  
Mode**

Template configuration mode

**Usage Guide**

 Make sure the IPv4 address is not pass-through.

**Configuration**

The following example configures 192.168.0.1 as the IPv4 address of the Wechat access device.

**Examples**

```
Hostname(config.tmplt.wechat)# nas-ip 192.168.0.1
```

**Platform**

N/A

**Description**

## 1.27 online-popup

Use this command to configure a post-login popup advertisement.

Use the **no** form of this command to restore the default setting.

**online-popup** *url-string*

**no online-popup**

**Parameter  
Description**

| Parameter         | Description |
|-------------------|-------------|
| <i>url-string</i> | Ad URL      |

**Defaults**

No post-login popup advertisement is configured by default.

**Command  
Mode**

Template configuration mode

**Usage Guide**

The URL of the popup advertisement should begin with "http://" or "https://".

**Configuration**

The following example configures a post-login popup advertisement.

**Examples**

```
Hostname(config.tmplt.iportal)# online-popup http://www.host.com
```

**Platform**

N/A

**Description**

## 1.28 page-suite

Use this command to configure a resource suite for the login page.

Use the **no** form of this command to restore the default setting.

**page-suite** *filename*

**no page-suite**

| Parameter<br>Description | Parameter       | Description         |
|--------------------------|-----------------|---------------------|
|                          | <i>filename</i> | Resource suite name |

**Defaults** The installed resource suite is used by default.

**Command Mode** Template configuration mode

**Usage Guide** Make sure to download page resource files in the directory of portal/zip under FLASH before.

**Configuration Examples** The following example configures a page suite for internal Web authentication.

```
Hostname(config.tmplt.iportal)#page-suite hostpage
```

**Platform Description** N/A

## 1.29 port

Use this command to set a surveillance port for the portal server.

Use the **no** form of this command to restore the default setting.

**port** { *port-num* }

**no port**

| Parameter<br>Description | Parameter   | Description                                                                                                                      |
|--------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------|
|                          | <i>port</i> | The surveillance port of the portal server, which is on only the 2nd generation portal server. The value ranges from 1 to 65535. |

**Defaults** The default is 50100 based on the UDP protocol.

**Command Mode** Template configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the surveillance port number of the eportalv2 server to 10000.

**Examples**

```
Hostname(config.tmplt.eportalv2)# port 10000
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.30 redirect

Use this command to set the redirect packet protocol.

Use the **no** form of this command to restore the default setting.

**redirect { http | js }**

**no redirect**

**Parameter  
Description**

| Parameter   | Description |
|-------------|-------------|
| <b>http</b> | HTTP 302    |
| <b>js</b>   | HTTP 200    |

**Defaults** Redirection packets of the Ruijie URL format use the JavaScript (JS) encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

**Command** Template configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the redirect packet protocol to HTTP 200.

**Examples**

```
Hostname(config.tmplt.eportalv2)# redirect http
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.31 service-url

Use this command to configure the URL of the authentication server for Wechat access.



**service-url** *url-string***no service-url****Parameter  
Description**

| Parameter         | Description                                        |
|-------------------|----------------------------------------------------|
| <i>url-string</i> | URL of the authentication server for Wechat access |




**Defaults**

No URL of the authentication server for Wechat access is configured by default.

**Command  
Mode**

Template configuration mode

**Usage Guide**

-  The URL can be configured in the format of either IP address or domain name. It cannot start with `http://` or `https://`. The configured `http://` or `https://` will be removed automatically.
-  It is required that only one IP address is resolved from the domain name.
-  After the domain name is configured, the IP address in the template will be overwritten by the IP address resolved from the domain name.

**Configuration**

The following example configures the URL of the authentication server for Wechat access.

**Examples**

```
Hostname(config.tmplt.wechat)# service-url wmc.hsot.com
```

**Platform**

N/A

**Description**

## 1.32 show web-auth acl

Use this command to display blacklists and whitelists.

**show web-auth acl** [ **black-ip** | **black-port** | **black-url** | **white-port** | **white-url** ]**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Command  
Mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration**

The following example displays blacklists and whitelists.

**Examples**

```
Hostname# show web-auth acl
Black URL List:0
```

```

-----
Black IP List:0
-----

White URL List:0
-----
    
```

**Platform** N/A  
**Description**

### 1.33 show web-auth control

Use this command to display controlled authentication configuration.

**show web-auth control**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example displays controlled authentication configurations.

```

Hostname(config)# show web-auth control
Port                Control  Server Name          Online User Count  Vlan Control List
-----
GigabitEthernet 0/1  On      <not configured>    0                  2-17, 19
Hostname(config)#
    
```

**Output Fields of the show web-auth control Command:**

| Field             | Description                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------|
| Port              | Name of a controlled port.                                                                        |
| Control           | Whether web authentication is enabled for a port.                                                 |
| Server Name       | Customized server name on the port. <not configured> indicates that no server name is configured. |
| Online User Count | Number of online users on a port.                                                                 |

**Prompt** N/A

**Platform Description** N/A

### 1.34 show web-auth direct-arp

Use this command to display the address range of the authentication-exempted ARP.

**show web-auth direct-arp**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** | N/A

**Configuration Examples** The following example displays the address range of the authentication-exempted ARP.

```

Hostname(config)# show web-auth direct-arp
Direct arps:
  Address      Mask
  -----
  1.1.1.1      255.255.255.255
  2.2.2.2      255.255.255.255
Hostname(config)#
    
```

| Field   | Description   |
|---------|---------------|
| Address | IPv4 address. |
| Mask    | IPv4 mask.    |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.35 show web-auth direct-host

This command is used to display the Web authentication-exempted users.

**show web-auth direct-host**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the Web authentication-exempted users.

### Examples

```

Hostname# show web-auth direct-host
Direct hosts:
  Address          Mask                Port      ARP Binding Group  Description
  -----
  192.168.0.1      255.255.255.255    Gi0/2     On      N/A      N/A
  192.168.4.11    255.255.255.255    Gi0/10    On      N/A      N/A
  192.168.5.0     255.255.255.0     Gi0/16    Off     N/A      N/A

```

| Field       | Description                                                 |
|-------------|-------------------------------------------------------------|
| Address     | IP address of the user free of authentication               |
| Mask        | IP address mask of the user free of authentication          |
| Port        | Access device port that is bound with the user's IP address |
| ARP Binding | Enable/Disable ARP binding                                  |
| Group       | Group which the user belongs to                             |
| Description | User description                                            |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

### 1.36 show web-auth direct site

Use this command to display the range of the Web authentication-exempted network resources.

**show web-auth direct-site**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults**

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the range of the Web authentication-exempted network resources without authentication.

```

Hostname (config) # show web-auth direct-site
Direct sites:
  Address      Mask           ARP Binding    Group    Descriptio
  -----
  1.1.1.1      255.255.255.255 Off           N/A      N/A
  2.2.2.2      255.255.255.255 On           N/A      N/A
Hostname (config) #
    
```

| Field       | Description                                           |
|-------------|-------------------------------------------------------|
| Address     | IP address.                                           |
| Mask        | IP mask.                                              |
| ARP Binding | Displays whether the ARP binding function is enabled. |
| Group       | Group which the network resource belongs to           |
| Description | Network resource description                          |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.37 show web-auth noise

Use this command to display the anti-noise configuration.

**show web-auth noise**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the anti-noise configuration.

### Examples

```

Hostname# show web-auth noise
Noise Enable:    On
  Aging Timer:   1min
  Hit Counts:    3
  
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.38 show web-auth parameter

Use this command to display the HTTP redirect configuration.

**show web-auth parameter**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the HTTP redirect configuration

**Examples**

```

Hostname# show web-auth parameter
  session-limit: 10
  timeout:      5
  
```

| Field         | Description                                                                |
|---------------|----------------------------------------------------------------------------|
| session-limit | Total number of HTTP sessions that are created by an unauthenticated user. |
| timeout       | Timeout interval of the redirection connection.                            |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.39 show web-auth portal-check

Use this command to display the portal-check configuration.

**show web-auth portal-check**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the portal-check configuration.

**Examples**

```

Hostname# show web portal-check
Check:      Enable
  Interval:  3s
  Timeout:   5s
  Retransmit: 3
Escape:     Enable
Nokick:     Disable
  
```

**Platform**  
**Description**

N/A

## 1.40 show web-auth rdport

Use this command to display the TCP interception port.

**show web-auth rdport**

**Parameter**  
**Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

N/A

**Command**  
**Mode**

Privileged EXEC mode

**Usage Guide**

N/A

**Configuration** The following example displays the TCP interception port.

**Examples**

```

Hostname# show web-auth rdport
Rd-Port:
80 443
Hostname#

```

**Related**  
**Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**  
**Description**

N/A

## 1.41 show web-auth syslog ip

Use this command to display user online and offline records

**show web-auth syslog ip** *ip-address*

**Parameter**  
**Description**

| Parameter         | Description                  |
|-------------------|------------------------------|
| <i>ip-address</i> | Indicates a user IP address. |

**Command**  
**Mode**

Privileged EXEC mode



**Default Level** 14

**Usage Guide** Use this command to display user online and offline records. This command does not store data before hot standby.

**Configuration** The following example displays online and offline records of a user:

**Examples**

```

Hostname# show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35 Core-index 0 Current index 2
Index:          0
Time:           2015-10-16 20:37:34
Behavior:       ONLINE
Mac:           00d0.f822.33e7
Vid:           101
Port:          Gi3/1
Timeused:      0d 00:00:00
Flow_up:       0
Flow_down:     0

Index:          1
Time:           2015-10-16 20:42:08
Behavior:       OFFLINE
Mac:           00d0.f822.33e7
Vid:           101
Port:          Gi3/1
Timeused:      0d 00:04:27
Flow_up:       2107872
Flow_down:     2108224

```

| Field     | Description                                              |
|-----------|----------------------------------------------------------|
| Index     | Record No                                                |
| Time      | Record occurrence time                                   |
| Behavior  | Online or offline action                                 |
| MAC       | MAC address of a user                                    |
| Vid       | VID of a user                                            |
| Port      | Port on the NAS used by user hosts to connect to the NAS |
| Timeused  | Online time                                              |
| Flow UP   | Uplink traffic of a user                                 |
| Flow down | Downlink traffic of a user                               |

**Prompt** N/A

**Platform**  
**Description** N/A

## 1.42 show web-auth template

Use this command to display the portal server configuration.

**show web-auth template**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the portal server configuration.

**Configuration** The following example displays the port server configuration.

### Examples

```

Hostname# show web-auth template
Webauth Template Settings:
-----
Name:      eportalv1
Url:       http://17.17.1.21:8080/eportal/index.jsp
Ip:        17.17.1.21
BindMode:  ip-mac-mode
Type:      v1
-----
Name:      eportalv2
Url:       http://17.17.1.21:8080/eportal/index.jsp
Ip:        17.17.1.21
BindMode:  ip-only-mode
Type:      v2
Port:      50100
Acctmlist:
Authmlist:
Hostname#

```

| Field | Description              |
|-------|--------------------------|
| Name  | Template name.           |
| Url   | Server homepage address. |
| Ip    | Server IP address.       |

|           |                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Type      | Server type, including the first generation portal server v1, the second generation portal server v2 and the intra portal server intra. |
| Port      | The protocol packet communication port of the server, which is on only the second generation portal server.                             |
| Acctmlist | Accounting method list name, which is on only the second generation portal server and the intra portal server                           |
| Authmlist | Authentication method list name. which is on only the second generation portal server and the intra portal server                       |

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.43 show web-auth user

Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.

**show web-auth user** { **all** | **ip** *ip-address* | **ip** *ipv6-address* | **mac** *mac-address* | **name** *name-string* | **escape** }

**Parameter  
Description**

| Parameter           | Description               |
|---------------------|---------------------------|
| <i>ip-address</i>   | IPv4 address of the user. |
| <i>ipv6-address</i> | IPv6 address of the user. |
| <i>mac-address</i>  | MAC address of the user.  |
| <i>name-string</i>  | User name.                |

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration  
Examples** The following example displays the global Web authentication configuration and statistics.

```

Hostname# show web-auth user all
Current user num : 4, online 2

Address           Online   Time Limit   Time Used   Status   Name

```

```
-----
192.168.0.11  On      0d 01:00:00  0d 00:15:10  Active
192.168.0.13  On      0d 01:00:00  0d 00:00:59  Active  111
192.168.0.25  Off     0d 01:00:00  0d 00:00:59  Create
192.168.0.46  Off     0d 01:00:00  0d 01:00:00  Destroy 222

Hostname# show web-auth user ip 192.168.0.11
Address      : 192.168.0.11
Mac          : 00d0.f800.2233
Port         : Gi0/2
Online       : On
Time Limit   : 0d 01:00:00
Time Used    : 0d 00:15:10
Time Start   : 2009-02-22 20:05:10
Status       : Active
```

| Field      | Description                                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address    | IP address of the user                                                                                                                                                         |
| Mac        | MAC address of the user                                                                                                                                                        |
| Port       | Access device port connected to the user                                                                                                                                       |
| Online     | Whether the user is online                                                                                                                                                     |
| Time Limit | Available duration of the user. 0 means unlimited.                                                                                                                             |
| Time Used  | Online duration of the user                                                                                                                                                    |
| Time Start | Time when the user passes authentication and gets online                                                                                                                       |
| Status     | User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared. |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

### 1.44 time-interval

Use this command to set the interval for popup advertisement.

Use the **no** form of this command to restore the default setting.

**time-interval** { hour }

**no time-interval**

**Parameter**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                               |                                                                             |
|-------------------------------|-----------------------------------------------------------------------------|
| <b>Description</b>            |                                                                             |
|                               | <i>hour</i>                                                                 |
|                               | The popup interval in the range from 0 to 24 in the unit of hours           |
| <b>Defaults</b>               | The default is 1 hour.                                                      |
| <b>Command Mode</b>           | Template configuration mode                                                 |
| <b>Usage Guide</b>            | If the parameter <i>hour</i> is 0, it means no popup interval.              |
| <b>Configuration Examples</b> | The following example sets the interval for popup advertisement to 2 hours. |
|                               | <pre>Hostname(config.tmplt.iportal)# time-interval 2</pre>                  |
| <b>Platform Description</b>   | N/A                                                                         |

## 1.45 url

Use this command to set the portal server URL.

Use the **no** form of this command to restore the default setting.

**url** *url-string*

**no url**

| Parameter Description | Parameter         | Description                                                                                                           |
|-----------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------|
|                       | <i>url-string</i> | Portal server URL, starting with <b>http://</b> or <b>https://</b> . The maximum length of this address is 255 bytes. |

**Defaults** No Portal server URL is configured for 1st, 2nd, iPortal, and WiFiDog authentication. In WeChat authentication template, the default Portal server URL is the redirection URL for coexistence of WeChat and SMS authentication on the MCP or WMC server.

**Command Mode** Template configuration mode

**Usage Guide** This command takes place of the **http redirect homepage [ url-string ]** command, which is now hidden as a compatible command.,  
If no URL is specified, the default URL in the **http://[ ip-address ]** format will be adopted, among which **ip-address** is the IP address of the server.

**Configuration Examples** The following example sets the eportalv1 template URL to **http://www.web-auth.net/login**.

```
Hostname(config.tmplt.eportalv1)# url http://www.web-auth.net/login
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A  
Description

## 1.46 webauth

Use this command to enable Web authentication.

Use the **no** form of this command to restore the default setting.

**webauth**

**no webauth**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

Defaults Web authentication is disabled by default.

Command Mode WLAN security configuration mode

Usage Guide N/A

Configuration The following example enables Web authentication.

Examples 

```
Hostname(config-wlansec)# webauth
```

Platform N/A  
Description

## 1.47 webauth prevent-jitter

Use this command to set the timeout for jitter prevention during Web authentication of a particular WLAN. Use the **no** or **default** form of this command to restore the default setting.

**webauth prevent-jitter** *timeout*

**no webauth prevent-jitter**

**default webauth prevent-jitter**

| Parameter Description | Parameter      | Description                                                                                                            |
|-----------------------|----------------|------------------------------------------------------------------------------------------------------------------------|
|                       | <i>timeout</i> | Sets the timeout for jitter prevention during Web authentication, in the range from 0 to 86400 in the unit of seconds. |

- Defaults** The default is 300 seconds.
- Command mode** WLAN security configuration mode
- Usage Guide** The jitter prevention time in Web authentication can be configured only after Web authentication is enabled.

**Configuration Examples** The following example sets the timeout for jitter prevention during Web authentication of WLAN 1 to 900 seconds.

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)# webauth
Hostname(config-wlansec)# webauth prevent-jitter 900

```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.48 web-auth accounting jitter-off

Use this command to enable jitter-off accounting function.  
Use **no** form of this command to restore the default setting.

**web-auth accounting jitter-off**

**no web-auth accounting jitter-off**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** Jitter-off accounting function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables jitter-off accounting function.

```

Hostname(config)# web-auth accounting jitter-off

```

**Platform**  
**Description**

N/A

## 1.49 web-auth accounting v2

Use this command to specify an accounting method.

Use **no** form of this command to restore the default setting.

**web-auth accounting v2** { **default** | *name* }

**no web-auth accounting v2** { **default** | *name* }

**Parameter**  
**Description**

| Parameter   | Description           |
|-------------|-----------------------|
| <i>name</i> | The accounting method |

**Defaults** No accounting method is specified by default.

**Command** Global configuration mode/ WLAN security configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example specifies an accounting method.

**Examples**

```
Hostname(config)# web-auth accounting v2 default
```

**Platform**  
**Description**

N/A

## 1.50 web-auth authentication v2

Use this command to specify an authentication method.

Use **no** form of this command to restore the default setting.

**web-auth authentication v2** [ **default** | *name* ]

**no web-auth authentication v2** [ **default** | *name* ]

**Parameter**  
**Description**

| Parameter   | Description               |
|-------------|---------------------------|
| <i>name</i> | The authentication method |

**Defaults** The default method is the same as AAA.

**Command** Global configuration mode/ WLAN security configuration mode  
**Mode**



**Usage Guide** N/A

**Configuration** The following example specifies an authentication method.

**Examples**

```
Hostname(config)# web-auth authentication v2 default
```

**Platform Description** N/A

## 1.51 web-auth acl

Use this command to configure a blacklist or whitelist.

Use **no** form of this command to restore the default setting.

**web-auth acl** { **black-ip** *black-ip* | **black-port** *black-port* | **black-url** *black-url* | **white-port** *white-port* | **white-url** *white-url* }

**no web-auth acl** { **black-ip** *ip* | **black-port** *port* | **black-url** *name* | **white-port** *port* | **white-url** *name* }

| Parameter Description | Parameter         | Description                                                   |
|-----------------------|-------------------|---------------------------------------------------------------|
|                       | <i>black-ip</i>   | Blacklist /Whitelist IP address                               |
|                       | <i>black-port</i> | Blacklist /Whitelist Port number in the range from 1 to 65535 |
|                       | <i>black-url</i>  | Blacklist /Whitelist URL                                      |
|                       | <i>white-url</i>  | Whitelist IP address                                          |
|                       | <i>white-port</i> | Whitelist port number in the range from 1 to 65,535           |

**Defaults** N/A

**Command Mode** Global configuration mode/WLAN security configuration mode

**Usage Guide** Use this command to configure a web authentication blacklist based on the port and URL and a whitelist based on the port.

**Configuration** The following example configures a blacklist and a whitelist.

**Examples**

```
Hostname(config)# web-auth acl black-ip 192.168.1.2
Hostname(config)# web-auth acl white-url www.ruijie.com.cn
```

**Platform Description** N/A

## 1.52 web-auth authen-mode

Use this command to configure IP address-based authentication, including IPv4, IPv6, and dual-stack

authentication. Use the **default** form of this command to restore the default setting.

**web-auth authen-mode** { ipv4 | ipv6 | both }


**default web-auth authen-mode**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           |             |

**Defaults** The default authentication mode is IPv4 authentication.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide**  If you want to configure dual-stack authentication, **ip dhcp snooping** must be enabled to allow the web authentication component to fetch the IPv4 address upon IPv6 authentication.

**Configuration Example** The following example configures the IPv6 authentication mode.

```
Hostname(config)# web-auth authen-mode ipv6
```

**Verification** Run the **show running-config** command to display the current configuration.

**Prompt** N/A

**Common Errors** N/A

**Platform Description** N/A

## 1.53 web-auth bind-portal

Use this command to bind MAC SMS authentication to the portal server.

Use **no** form of this command to restore the default setting.

**web-auth bind-portal** *string type* { local-spec | group-spec }

**no web-auth bind-portal**

| Parameter Description | Parameter     | Description        |
|-----------------------|---------------|--------------------|
|                       | <i>string</i> | Portal server name |

**Defaults** N/A

**Command** WLAN security configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example binds MAC SMS authentication to the portal server.

**Examples**

```
Hostname(config-wlansec)# web-auth bind-portal eportalv2 type group-sec
```

**Platform**  
**Description** N/A

## 1.54 web-auth dhcp-check

Use this command to enable DHCP IP address check.

Use **no** form of this command to restore the default setting.

**web-auth dhcp-check**

**no web-auth dhcp-check**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** DHCP IP address check is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** Only users whose IP addresses are allocated by DHCP are allowed to take authentication.

**Configuration** The following example enables DHCP IP address check.

**Examples**

```
Hostname(config)# web-auth dhcp-check
```

**Platform**  
**Description** N/A

## 1.55 web-auth direct-host

Use this command to set the authentication-exempted IP/MAC address range.

Use the **no** form of this command to restore the default setting.

**web-auth direct-host** { *ipv4-address* [ *ip-mask* ] [ **arp** ] | *ipv6-address* | *mac-address* } [ **port** *interface-name* ]

**no web-auth direct-host** { *ipv4-address* [ *ip-mask* ] | *ipv6-address* | *mac-address* }

| Parameter Description | Parameter                         | Description                                                                                                                                                                                     |
|-----------------------|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>ipv4-address</i>               | IPv4 address of authentication-exempted user                                                                                                                                                    |
|                       | <i>ipv6-address</i>               | IPv6 address of authentication-exempted user                                                                                                                                                    |
|                       | <i>ip-mask</i>                    | Mask of the IPv4 address free of authentication (optional).                                                                                                                                     |
|                       | <b>port</b> <i>interface-name</i> | Binds user's IP address with a port of the access device (optional).                                                                                                                            |
|                       | <b>arp</b>                        | If ARP CHECK is enabled on the access device, keyword arp is needed for ARP binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only. |
|                       | <i>mac-address</i>                | MAC address of authentication-exempted user                                                                                                                                                     |

**Defaults** No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.

**Command Mode** Global configuration mode

**Usage Guide** When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication.  
Up to 50 users can be set to be exempted from authentication.

**Configuration Examples** The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication.

```
Hostname(config)# web-auth direct-host 172.16.0.1
```

The following example sets the user with the IPv6 address FF02::/64 to be exempted from authentication.

```
Hostname(config)# web-auth direct-host FF02::/64
```

| Related Commands | Command                          | Description                                    |
|------------------|----------------------------------|------------------------------------------------|
|                  | <b>show web-auth direct-host</b> | Displays the users free of Web authentication. |

**Platform Description** N/A

## 1.56 web-auth dkey-compatible url-parameter

Use this command to configure the DKEY-compatible URL string.

Use the **no** form of this command to restore the default setting.

**web-auth dkey-compatible url-parameter** *string*

**no web-auth dkey-compatible url-parameter**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |               |                            |
|--------------------|---------------|----------------------------|
| <b>Description</b> |               |                            |
|                    | <i>string</i> | DKEY-compatible URL string |

**Defaults** The DKEY-compatible URL string is not configured by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example configures the DKEY-compatible URL string as login.

**Examples**

```
Hostname(config)# web-auth dkey-compatible url-parameter login
```

| <b>Related Commands</b> | Command | Description |
|-------------------------|---------|-------------|
|                         | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.57 web-auth linkdown-timeout

Use this command to configure the authenticated user logout delay after a port is Down. Use the **no** form of this command to remove the configuration.

**web-auth linkdown-timeout** { *timeout* }

**no web-auth linkdown-timeout**

| <b>Parameter Description</b> | Parameter      | Description                                                                                             |
|------------------------------|----------------|---------------------------------------------------------------------------------------------------------|
|                              | <i>timeout</i> | Authenticated user logout delay after a port is down, in seconds. The value range is from 1 to 604,800. |

**Defaults** 60s

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** N/A

**Configuration** The following example sets the authenticated user logout delay after a port is down to 11 seconds :

**Examples**

```
Hostname(config)# web-auth linkdown-timeout 11
```

|                             |                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------|
| <b>Verification</b>         | Run the <b>show running-config</b> command to display the current configuration. |
| <b>Prompt</b>               | N/A                                                                              |
| <b>Common Errors</b>        | N/A                                                                              |
| <b>Platform Description</b> | N/A                                                                              |

## 1.58 web-auth logging enable

Use this command to enable the Web authentication syslog function.

Use the **no** form of this command to restore the default setting.

**web-auth logging enable** { *num* }

**no web-auth logging enable**

| <b>Parameter Description</b> | Parameter  | Description                                                                                                                                             |
|------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | <i>num</i> | The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 100. 0 indicates no limit. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to limit the syslog printing rate for only the functional module.

**Configuration Examples** The following example enables the syslog printing with no rate limit.

```
Hostname(config)# web-auth logging enable 0
```

| <b>Related Commands</b> | Command | Description |
|-------------------------|---------|-------------|
|                         | N/A     | N/A         |

**Platform Description** N/A

## 1.59 web-auth noise

Use this command to configure the anti-noise policy.

Use the no form of this command to restore the default setting.

**web-auth noise** [ **aging** *agmin* ] [ **hit** *times* ]

**no web-auth noise**

| Parameter Description | Parameter    | Description                                                                                                                         |
|-----------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>agmin</i> | Anti-noise aging time in the range from 1 to 30 in the unit of minutes. The default is 1 minute.                                    |
|                       | <i>times</i> | Anti-noise time limit in the range from 3 to 100. The default is 3. IP addresses accessing for the time limit are thought as noise. |

**Defaults** The anti-noise policy is not configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the anti-noise policy.

**Examples**

```
Hostname(config)# web-auth noise aging 1 hit 3
```

**Platform** N/A  
**Description**

## 1.60 web-auth offline-detect

Use this command to configure the online keepalive time for users. Authenticated online users are forced to go offline if their traffic is lower than the specified threshold within a specified interval.

**web-auth offline-detect interval** *interval* **flow** *threshold*

Use this command to restore the default setting.

**default web-auth offline-detect**

Use this command to disable online detection for users.

**no web-auth ping**

| Parameter Description | Parameter       | Description                                                                                             |
|-----------------------|-----------------|---------------------------------------------------------------------------------------------------------|
|                       | <i>interval</i> | The offline detection interval. The value ranges from 1 min to 65,535 min. The default value is 10 min. |

|                  |                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>threshold</i> | The traffic threshold. The value ranges from 0 bytes to 4,294,967,294 bytes. The default value is 0, indicating that traffic detection is not performed. |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** 15min

**Command Mode** WLANSEC configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures user detection under WLANSEC 1. If users' traffic is lower than 5k Bytes within 5minutes, they are forced to go offline.

```

Hostname(config)# wlansec 1
Hostname(config-wlansec)# web-auth offline-detect interval 5 flow 5120

```

**Verification** Run the **show running** command to display corresponding configuration of online detection for users.

**Platform Description** N/A

## 1.61 web-auth ping

Use this command to ping the portal server.

Use the no form of this command to restore the default setting.

**web-auth ping** [ *interval minutes* | *retry times* ]

**no web-auth ping**

| Parameter Description | Parameter      | Description                                                                                   |
|-----------------------|----------------|-----------------------------------------------------------------------------------------------|
|                       | <i>minutes</i> | Ping interval in the range from 1 to 65,535 in the unit of minute<br>The default is 1 minute. |
|                       | <i>times</i>   | Ping retries in the range from 0 to 65,535<br>The default is 3.                               |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command must be used with the **fmt** command. Before using this command, run the **fmt** command to configure the URL format. Otherwise, this command does not take effect.



**Configuration** The following example configures ping interval as 5 minutes and retries as 4.

**Examples**

```
Hostname(config)# web-auth ping interval 5 rerty 4
```

**Platform**  
**Description** N/A

## 1.62 web-auth portal

Use this command to map different portal servers with users in different subnets.

Use the **no** form of this command to restore the default setting.

**web-auth portal** { **eportalv1** | **eportalv2** | **iportal** | **wechat** | **wifidog** | *name* }

**no web-auth portal** { **eportalv1** | **eportalv2** | **iportal** | **wechat** | **wifidog** | *name* }

| Parameter Description | Parameter   | Description        |
|-----------------------|-------------|--------------------|
|                       | <i>name</i> | Portal server name |

**Defaults** This function is disabled by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the WeChat server.

**Examples**

```
Hostname(config)# web-auth portal wechat
```

The following example configures the WiFiDog server.

```
Hostname(config)# web-auth portal wifidog
```

**Platform**  
**Description** N/A

## 1.63 web-auth portal extension

Use this command to enable portal extension to support CMCC portal server.

Use the **no** form of this command to restore the default setting.

**no web-auth portal extension**

**default web-auth portal extension**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** By default, Ruijie portal server is supported.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example disables portal extension.

**Examples**

```

Hostname(config)# no web-auth portal extension
Hostname(config)# http redirect url-fmt ext1

```

**Platform Description** N/A

## 1.64 web-auth portal key

Use this command to set the communication key between the access device and the authentication server.

Use the **no** form of this command to clear the communication key between the redirected Web request of a user and the authentication server.

**web-auth portal key** *key-string*

**no web-auth portal key**

| Parameter Description | Parameter         | Description                                                                                                            |
|-----------------------|-------------------|------------------------------------------------------------------------------------------------------------------------|
|                       | <i>key-string</i> | Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes. |

**Defaults** No key is set by default.

**Command Mode** Global configuration mode

**Usage Guide** To use the Web authentication function, the communication key between the access device and the authentication server must be set.

**Configuration Examples** The following example sets the communication key between the access device and the authentication server to web-auth.

```

Hostname(config)# web-auth portal key web-auth

```

| Related Commands | Command              | Description                                       |
|------------------|----------------------|---------------------------------------------------|
|                  | <b>http redirect</b> | Sets the IP address of the authentication server. |

|                               |                                                  |
|-------------------------------|--------------------------------------------------|
| <b>http redirect homepage</b> | Sets the address of the authentication homepage. |
| <b>web-auth port-control</b>  | Enables the Web authentication on the port.      |

**Platform** N/A

**Description**

## 1.65 web-auth portal-attribute

Use this command to configure transparent transmission of the 0x05 attribute of the portal protocol.

Use the **no** form of this command to restore the default setting.

**web-auth portal-attribute** { 5 | textinfo }

**no web-auth portal-attribute** { 5 | textinfo }

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

**Command  
Mode** Global configuration mode

**Usage Guide** In general, enable this function on the portal server when a device needs to upload the error flag (ErrID), or enable this function on the portal server (using Huawei portal protocol 2.0) when a device needs to upload prompts (TextInfo) from a third-party authentication device such as the RADIUS server.

**Configuration  
Examples** Both of the following examples configure transparent transmission of the 0x05 attribute of the portal protocol.

```
Hostname(config)# web-auth portal-attribute 5
Hostname(config)# web-auth portal-attribute textinfo
```

**Platform  
Description** N/A

## 1.66 web-auth portal-check

Use this command to enable portal server check.

Use the **no** form of this command to restore the default setting.

**web-auth portal-check** [ interval *intsec* ] [ timeout *tosec* ] [ retransmit *retires* ]


**no web-auth porta-check**


| Parameter Description | Parameter      | Description                                                                                        |
|-----------------------|----------------|----------------------------------------------------------------------------------------------------|
|                       | <i>Intsec</i>  | Check interval in the range from 1 to 1,000 in the unit of seconds.<br>The default is 10 seconds.  |
|                       | <i>tosec</i>   | Timeout interval in the range from 1 to 1,000 in the unit of seconds.<br>The default is 5 seconds. |
|                       | <i>retries</i> | Retry count in the range from 1 to 100.<br>The default is 3.                                       |

**Defaults** Portal server check is disabled by default.

**Command Mode** Global configuration mode

#### Usage Guide

 In most networks, only one server is deployed and this function does not need to be configured. If multiple portal servers exist, it is recommended that the detection interval and packet timeout time not be set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

 This command cannot be used with the **fmt** command. If you want to use the **fmt** command to configure the URL format, run the **web-auth ping** command for Portal server detection.

**Configuration** The following example enables portal server check.

**Examples**

```
Hostname(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

**Platform** N/A  
**Description**

## 1.67 web-auth portal-escape

Use this command to enable portal-escape function.

Use the **no** form of this command to restore the default setting.

**web-auth portal-escape [ nokick ]**

**no web-auth portal-escape**

| Parameter Description | Parameter     | Description                                                                                                            |
|-----------------------|---------------|------------------------------------------------------------------------------------------------------------------------|
|                       | <b>nokick</b> | Configures not to force online users offline if the portal server is unavailable after the escape function is enabled. |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** Use this command together with **web-auth portal-check** command to sustain key services when the portal server is abnormal.

**Configuration** The following example enables portal-escape function.

**Examples** `Hostname(config)# web-auth portal-escape`

**Platform** N/A  
**Description**

## 1.68 web-auth portal-valid unique-name

Use this command to enable uniqueness check of portal authentication accounts.

Use the **no** form of this command to restore the default setting.

**web-auth portal-valid unique-name**


**no web-auth portal-vallid unique-name**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide**  Enable this feature when the portal server is needed to send preemption prompts to users.

**Configuration** The following example enables uniqueness check of portal authentication accounts.

**Examples** `Hostname(config)# web-auth portal-valid unique-name`

**Platform** N/A  
**Description**

## 1.69 web-auth sms-flow

Use this command to configure the interval and threshold of flow detection.

Use the **no** form of this command to restore the default setting.

**web-auth sms-flow [ interval *interval* ] [ threshold *flows* ]**

**no web-auth sms-flow [ interval *interval* ] [ threshold *flows* ]**

|                               |                                                                                |                                                                    |
|-------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                               | <b>Description</b>                                                 |
|                               | <i>interval</i>                                                                | Detection interval in minutes. The value ranges from 1 to 65,535.  |
|                               | <i>flows</i>                                                                   | Traffic threshold in KB. The value ranges from 0 to 4,294,967,295. |
| <b>Defaults</b>               | No interval and threshold is configured by default.                            |                                                                    |
| <b>Command Mode</b>           | Global configuration mode                                                      |                                                                    |
| <b>Usage Guide</b>            |                                                                                |                                                                    |
| <b>Configuration Examples</b> | The following example configures the interval and threshold of flow detection. |                                                                    |
|                               | <pre>Hostname(config)# web-auth sms-flow interval 5 threshold 100</pre>        |                                                                    |
| <b>Platform Description</b>   | N/A                                                                            |                                                                    |

## 1.70 web-auth sta-leave detection

Use this command to disable STA connectivity detection.

**no web-auth sta-leave detection**

Use this command to restore the default setting.

**default web-auth sta-leave detection**

|                               |                                                              |                    |
|-------------------------------|--------------------------------------------------------------|--------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                             | <b>Description</b> |
|                               | N/A                                                          | N/A                |
| <b>Defaults</b>               | The STA connectivity detection is enabled by default.        |                    |
| <b>Command Mode</b>           | Global configuration mode                                    |                    |
| <b>Usage Guide</b>            |                                                              |                    |
| <b>Configuration Examples</b> | The following example disables STA connectivity detection.   |                    |
|                               | <pre>Hostname(config)# no web-auth sta-leave detection</pre> |                    |
| <b>Platform Description</b>   | N/A                                                          |                    |

## 1.71 web-auth sta-perception enable

Use this command to enable smart authentication for Wechat access.

Use the **no** form of this command to restore the default setting.

**web-auth sta-perception enable**

**no web-auth sta-perception enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode or WLAN security configuration mode

**Usage Guide** N/A

**Configuration** The following example enables smart authentication for Wechat access.

**Examples**

```
Hostname(config)# web-auth sta-perception enable
```

**Platform Description** N/A

## 1.72 web-auth template

Use this command to create the first generation authentication template and enter its configuration mode.

**web-auth template eportalv1**

Use this command to create the customized first generation authentication template and enter its configuration mode.

**web-auth template { template-name } v1**

Use this command to create the second generation authentication template and enter its configuration mode.

**web-auth template eportalv2**

Use this command to create the customized second generation authentication template and enter its configuration mode.

**web-auth template { template-name } v2**

Use this command to create the built-in authentication template and enter its configuration mode.

**web-auth template iportal**

Use this command to create the customized built-in authentication template and enter its configuration mode.

**web-auth template** { template-name } **intra**

Use this command to create the WiFiDog authentication template and enter its configuration mode.

**web-auth template wifidog**

Use this command to create the customized WiFiDog authentication template and enter its configuration mode.

**web-auth template** { template-name } **wifidog**

Use this command to create the Wechat authentication template and enter its configuration mode.

**web-auth template wechat**

Use this command to create the customized Wechat authentication template and enter its configuration mode.

**web-auth template** { template-name } **wechat**

Use this command to create and enter the default clearpass authentication template configuration mode.

**web-auth template cpweb**

Use this command to create and enter the custom clearpass authentication template configuration mode.

**web-auth template** { template-name } **cpweb**

Use this command to create and enter the default app authentication template configuration mode.

**web-auth template app**

Use this command to create and enter the custom app authentication template configuration mode.

**web-auth template** { template-name } **app**

Use this command to remove the template.

**no web-auth template** { *template-name* }

**Parameter  
Description**

| Parameter        | Description                                            |
|------------------|--------------------------------------------------------|
| <b>eportalv1</b> | Applies the first generation authentication template.  |
| <b>eportalv2</b> | Applies the second generation authentication template. |
| <b>iportal</b>   | Applies the built-in authentication template.          |
| <b>wechat</b>    | Applies the Wechat authentication template.            |
| <b>wifidog</b>   | Applies the WiFiDog authentication template.           |



|                      |                                                          |
|----------------------|----------------------------------------------------------|
| <b>wechat</b>        | Applies the default WeChat authentication template.      |
| <b>cpweb</b>         | Applies the default clearpass authentication template.   |
| <b>app</b>           | Applies the default app authentication template.         |
| <i>template-name</i> | Sets the name of the customized authentication template. |

**Defaults** No template is configured by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** You can enter the **eportalv1** template mode to configure the IP address and URL instead of executing the **http redirect** and **http redirect homepage** commands. The **http redirect** and **http redirect homepage** commands are compatible on the device, which will be converted to this command. The original command **portal-server** is compatible on the device, which will be converted to this command.

To ensure the Web authentication function, configure and apply a functional portal server. The **eportalv1** template is applied by default. The IP address, the URL and the communication secret key of the **eportalv1** template should be configured. If no URL format is specified, the default **http://[ ip-address ]** format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.

**Configuration** The following example configures the **eportalv1** template.

**Examples**

```
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)#
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.73 web-auth update-interval

Use this command to set the interval at which the online user information is updated.

Use the **no** form of this command to restore the default setting.

**web-auth update-interval** {seconds}

**no web-auth update-interval**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                |                                                                                   |
|----------------|-----------------------------------------------------------------------------------|
| <i>seconds</i> | Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds. |
|----------------|-----------------------------------------------------------------------------------|

**Defaults** The default is 180 seconds.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the interval at which the online user information is updated to 60 seconds.

```
Hostname(config)# web-auth update-interval 60
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.74 web-auth valid-ip-acct

Use this command to configure the time during which STAs can attempt to obtain IP addresses. The STAs that fail to obtain IP addresses after the specified time has elapsed are forced offline.

**web-auth valid-ip-acct [ timeout *seconds* ]**


Use this command to restore the default setting.

**no web-auth valid-ip-acct**

| Parameter Description | Parameter      | Description |
|-----------------------|----------------|-------------|
|                       | <i>seconds</i> |             |

**Defaults** By default, smart IP address check is not configured.

**Command Mode** Global configuration mode

**Usage Guide**  The configuration only works to users of smart authentication for WeChat access.

**Configuration Examples** Use this command to configure the time as 1min.

```
Hostname(config)# web-auth valid-ip-acct timeout 60
```

**Platform**  
**Description**

N/A

## 1.75 web-auth wechat-check

Use this command to configure detection of the authentication server for WeChat access.

Use the **no** form of this command to restore the default setting.

**web-auth wechat-check interval** *minutes*

**no web-auth wechat-check**


**Parameter**  
**Description**

| Parameter      | Description                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------|
| <i>minutes</i> | Interval for server detection. It is recommended to set it to 30 minutes. The value ranges from 1 to 65535. |

**Defaults** Server detection is not configured by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide**

 Server detection teams up with collective escape. Run the **web-auth wechat-escape interval** *minutes* **times** *count* command to enable collective escape.

**Configuration** The following example configures the interval for server detection.

**Examples**

```
Hostname(config)# web-auth wechat-check interval 30
```

**Platform**  
**Description**

N/A

## 1.76 web-auth wechat-escape

Use this command to enable collective escape of the authentication server for WeChat access.

**web-auth wechat-escape interval** *minutes* **times** *times*

Use the **no** form of this command to disable collective escape.

**no web-auth wechat-check**


Use this command to cancel collective escape and resume single escape. As a trigger, it is not displayed when running the **show running-config** command.

**web-auth wechat-escape recover**

| Parameter Description | Parameter      | Description                                                                     |
|-----------------------|----------------|---------------------------------------------------------------------------------|
|                       | <i>minutes</i> | Escape interval. By default, it is 60minutes. The value ranges from 1 to 65535. |
|                       | <i>times</i>   | Number of escape times. The value ranges from 1 to 65,535.                      |
|                       |                |                                                                                 |

**Defaults** Collective escape is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide**  After you clear escape status by running the **web-auth wechat-escape recover** command, the escape status will be resumed if the server is still unreachable.

**Configuration** The following example configures the parameters for collective escape.

**Examples**

```
Hostname(config)# web-auth wechat-escape interval 30 times 10
```

**Platform Description** New feature in wlansec configuration mode in release RGOS11.1(5)B23 and later.

## 1.77 web-auth wechat-template wlan-range portal-ip nas-ip

Use this command to enable the one-click switch configuration via WeChat.

**web-auth wechat-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* [ **escape** | **nas-id** *nas-id* | **ios-adapter** | **perception** ]

Use the **no** form of this command to disable the one-click switch configuration via WeChat.

**no web-auth wechat-template** *name*

| Parameter Description | Parameter                   | Description                                                                                                                                         |
|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>name</i>                 | Indicates the template name.                                                                                                                        |
|                       | <i>wlanid-start</i>         | Indicates the start WLAN ID.                                                                                                                        |
|                       | <i>wlanid-end</i>           | Indicates the end WLAN ID.                                                                                                                          |
|                       | <i>portal-ip-addr</i>       | Indicates the IP address of the portal server.                                                                                                      |
|                       | <i>nas-ip-addr</i>          | Sets the IP address for a device with WeChat configured to access a service, so that the server sends packets to this IP address for communication. |
|                       | <b>escape</b>               | Escape.                                                                                                                                             |
|                       | <b>nas-id</b> <i>nas-id</i> | Sets the AC's NAS ID. It is mandatory in hot standby and VAC scenarios, which present multiple devices as one.                                      |
|                       | <b>ios-adapter</b>          | Enables automatic popups.                                                                                                                           |

|                   |                                      |
|-------------------|--------------------------------------|
| <b>perception</b> | Enables the non-perception function. |
|-------------------|--------------------------------------|



**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Default Level** 14

#### Usage Guide

-  The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.
-  The NAS ID configuration applies to only hot standby and VAC scenarios. It is not required by the standalone scenario.

**Configuration** The following example enables the one-click switch configuration.

#### Examples

```
Hostname(config)# web-auth wechat-template aaa wlan-range 2 5 portal-ip
172.21.6.78 nas-ip 192.168.197.227
```

#### Verification

## 1.78 web-auth wifidog-template wlan-range portal-ip nas-ip url

Use this command to enable the one-click switch configuration via WiFiDog.

**web-auth wifidog-template** *name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-addr* **nas-ip** *nas-ip-addr* **url** *url-string* [ **escape** | **gateway-id** *gwid-str* | **perception** ]

Use the **no** form of this command to disable the one-click switch configuration via WiFiDog.

**no web-auth wifidog-template** *name*

#### Parameter Description

| Parameter             | Description                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>name</i>           | Indicates the template name.                                                                                                                         |
| <i>wlanid-start</i>   | Indicates the start WLAN ID.                                                                                                                         |
| <i>wlanid-end</i>     | Indicates the end WLAN ID.                                                                                                                           |
| <i>portal-ip-addr</i> | Indicates the IP address of the portal server.                                                                                                       |
| <i>nas-ip-addr</i>    | Sets the IP address for a device with WiFiDog configured to access a service, so that the server sends packets to this IP address for communication. |
| <i>url-string</i>     | Indicates the URL for portal server authentication.                                                                                                  |
| <b>escape</b>         | Escape.                                                                                                                                              |
| <i>gwid-str</i>       | Sets the serial number. It is mandatory in hot standby and VAC scenarios, which present multiple devices as one.                                     |
| <b>gateway-id</b>     | Config gateway id.                                                                                                                                   |
| <b>perception</b>     | Enables the non-perception function.                                                                                                                 |



**Defaults** N/A

**Command** Global configuration mode

**Mode**

**Default Level** 14

**Usage Guide**

-  The one-click configuration function can control only one port at a time. To control multiple ports, perform one-click configuration for the required times. The **no** form of this command can delete template information and all the controlled ports, but is not globally valid.
-  The gateway ID configuration applies to only hot standby and VAC scenarios. It is not required by the standalone scenario.

**Configuration** The following example enables the one-click switch configuration via WiFiDog.

**Examples**

```
Hostname (config) # web-auth wifidog-template aaa interface tenGigabitEthernet 3/2
portal-ip 172.21.6.78 nas-ip 192.168.197.227 url
http://172.21.6.78/auth/wifidogAuth
```

**Verification** Run the **show running-config** command to display the current configurations.

## 1.79 web-auth winterface

Use this command to configure the winterface parameter in redirect URL.

Use the **no** form of this command to restore the default setting.

**web-auth winterface** *string*

**no web-auth winterface**

**Parameter  
Description**

| Parameter     | Description          |
|---------------|----------------------|
| <i>string</i> | winterface parameter |

**Defaults** The winterface parameter is not configured by default.

**Command** WLAN security configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example configures the winterface parameter in redirect URL.

**Examples**

```
Ruijie (wlansec) # web-auth winterface winterface
```

**Platform**

**Description**

N/A

## 1.80 web-auth wlan-ac-ip

Use this command to configure the ACIP parameter in redirect URL.

Use the **no** form of this command to restore the default setting.

**web-auth wlan-ac-ip** *ipv4*

**no web-auth wlan-ac-ip**

| Parameter<br>Description | Parameter   | Description    |
|--------------------------|-------------|----------------|
|                          | <i>ipv4</i> | ACIP parameter |

**Defaults** The ACIP Parameter is not configured by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures the ACIP parameter in redirect URL.

```
Hostname(config-wlansec)# web-auth wlan-ac-ip 192.168.1.100
```

**Platform Description** N/A

# 1 SCC Commands

## 1.1 downstream average-rate burst-rate

Use this command to configure the downstream traffic average and burst threshold. Use the **no** form of this command to remove the configuration.

**downstream average-rate** *avg-threshold* **burst-rate** *burst-threshold*  
**no downstream**

| Parameter Description | Parameter              | Description                                                            |
|-----------------------|------------------------|------------------------------------------------------------------------|
|                       | <i>avg-threshold</i>   | Indicates the traffic average, in the range from 8 to 261,120.         |
|                       | <i>burst-threshold</i> | Indicates the traffic burst threshold, in the range from 8 to 261,120. |

**Defaults** N/A

**Command Mode** Speed-limit strategy configuration mode

**Default Level** 14

**Usage Guide** The burst thresholds of downstream parameters must not be smaller than the average.

**Configuration** The following example configures the downstream traffic average and burst threshold.

**Examples**

```

Hostname(config)# rate-policy user-rate
Hostname(config-rate-policy)# downstream average-rate 10 burst-rate 10

```

**Verification** Use the **show running** command to display the speed-limit downstream policy rule.

**Prompt** N/A

**Common Errors** N/A

**Platform**

## 1.2 filter-acl

Use this command to configure the security ACL associated with the filtering policy. Use the **no** form of this command to remove the configuration.

**filter-acl** { *acl-name* | *acl-id* }



**no filter-acl**

| Parameter Description         | Parameter                                                                                                                                                        | Description                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|                               | <i>acl-name</i>                                                                                                                                                  | Indicates the name of the security ACL associated with the filtering policy. |
|                               | <i>acl-id</i>                                                                                                                                                    | Indicates the ID of the security ACL associated with the filtering policy.   |
| <b>Defaults</b>               | N/A                                                                                                                                                              |                                                                              |
| <b>Command Mode</b>           | Filtering policy configuration mode                                                                                                                              |                                                                              |
| <b>Default Level</b>          | 14                                                                                                                                                               |                                                                              |
| <b>Usage Guide</b>            | One filtering policy can be deployed in different service strategies.                                                                                            |                                                                              |
| <b>Configuration Examples</b> | The following example configures a filtering policy.                                                                                                             |                                                                              |
|                               | <pre> Hostname(config)# ip access-list extended user_2000 Hostname(config)# filter-policy user-filter Hostname(config-filter-policy)#filter-acl user_2000 </pre> |                                                                              |
| <b>Verification</b>           | Use the <b>show running</b> command to display the security ACL associated with the filtering policy.                                                            |                                                                              |
| <b>Prompt</b>                 | N/A                                                                                                                                                              |                                                                              |
| <b>Common Errors</b>          | N/A                                                                                                                                                              |                                                                              |
| <b>Platform</b>               | N/A                                                                                                                                                              |                                                                              |

## 1.3 filter-policy

Use this command to enter filtering policy configuration mode. Use the **no** form of this command to remove the configuration.

**filter-policy** *filter-name*

**filter-acl** { *acl-name* | *acl-id* }

| Parameter Description | Parameter          | Description                                                                  |
|-----------------------|--------------------|------------------------------------------------------------------------------|
|                       | <i>filter-name</i> | Indicates the name of a filtering policy.                                    |
|                       | <i>acl-name</i>    | Indicates the name of the security ACL associated with the filtering policy. |
|                       | <i>acl-id</i>      | Indicates the ID of the security ACL associated with the filtering           |

|  |         |
|--|---------|
|  | policy. |
|--|---------|

- Defaults** N/A
- Command Mode** Global configuration mode
- Default Level** 14
- Usage Guide** One filtering policy can be deployed in different service strategies.

**Configuration** The following example configures a filtering policies.

**Examples**

```

Hostname(config)# ip access-list extended user_2000
Hostname(config)# filter-policy user-filter
Hostname(config-filter-policy)# filter-acl user_2000
    
```

- Verification** Use the **show running** command to display the filtering configuration policy.
- Prompt** N/A
- Common Errors** N/A

**Platform**

## 1.4 filter-policy apply

Use this command to configure the filtering policy. Use the **no** form of this command to remove the configuration.

**filter-policy** *filter-name* **apply**

**no filter-policy**

| Parameter Description | Parameter          | Description                                            |
|-----------------------|--------------------|--------------------------------------------------------|
|                       | <i>filter-name</i> | Indicates the name of the filtering policy to be used. |

**Defaults**

- Command Mode** User policy configuration mode
- Default Level** 14
- Usage Guide** The name of the filtering policy to be used should be configured first.

**Configuration** The following example configures a user policy and specifies the filtering policy name.

**Examples**

```

Hostname(config)# ip access-list extended user_2000
    
```

```

Hostname(config)# filter-policy user-filter
Hostname(config-filter-policy)# filter-acl user_2000
Hostname(config)# service-policy user-policy
Hostname(config-service-policy)# filter-policy user-filter apply

```

**Verification** Use the **show running** command to display the filtering policy to be used.

**Prompt** N/A

**Common Errors** N/A

**Platform**

## 1.5 offline-detect interval threshold

Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval. Use the **no** or **default** form of this command to restore the default setting.

**offline-detect interval** *interval* **threshold** *threshold*

**default offline-detect**

**no offline-detect**

**Parameter  
Description**

| Parameter        | Description                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interval</i>  | Indicates the interval of traffic detection (in minutes). The range is from 1 to 65,535 in minutes.                                                                                        |
| <i>threshold</i> | Indicates the traffic threshold (in bytes). The range is from 0 to 4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected. |

**Defaults** By default, the detection interval is 8 hours and the traffic threshold is 0.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.

**Configuration Examples** The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes.

```

Hostname(config)#offline-detect interval 5 threshold 5120

```

**Verification** Use the **show running** command to display the configuration of online-status detection for authenticated users.

**Prompt** N/A

**Common Errors** N/A

**Platform** N/A

## 1.6 rate-policy

Use this command to enter speed-limit policy configuration mode.

**rate-policy** *rate-name*

Use this command to configure the upstream traffic average and burst threshold.

{ **downstream** | **upstream** } **average-rate** *avg-threshold* **burst-rate** *burst-threshold*

| Parameter Description | Parameter              | Description                                                            |
|-----------------------|------------------------|------------------------------------------------------------------------|
|                       | <i>rate-name</i>       | Indicates the name of a speed-limit policy.                            |
|                       | <i>avg-threshold</i>   | Indicates the traffic average, in the range from 8 to 261,120.         |
|                       | <i>burst-threshold</i> | Indicates the traffic burst threshold, in the range from 8 to 261,120. |

**Command Mode** Speed-limit strategy configuration mode

**Level** 14

**Usage Guide** One speed-limit policy can be deployed in different service strategies.

**Configuration Examples** The following example configures the upstream traffic average and burst threshold.

```

Hostname(config)# rate-policy user-rate
Hostname(config-rate-policy)#upstream average-rate 10 burst-rate 10
Hostname(config-rate-policy)#downstream average-rate 10 burst-rate 10

```

**Verification** Run the **show running** command to display the speed limit policy.

**Prompt** N/A

**Platform**

## 1.7 rate-policy apply

Use this command to configure the speed-limit policy to be used. Use the **no** form of this command to remove the configuration.

**rate-policy** *rate-name* **apply**

**no rate-policy**

### Parameter Description

| Parameter        | Description                                              |
|------------------|----------------------------------------------------------|
| <i>rate-name</i> | Indicates the name of the speed-limit policy to be used. |

**Command Mode** User policy configuration mode

**Level** 14

**Usage Guide** The name of the speed-limit policy to be used should be configured first.

**Configuration Examples** The following example configures the speed-limit policy to be used and specifies the policy name.

```

Hostname(config)# rate-policy user-rate
Hostname(config-rate-policy)#upstream average-rate 10 burst-rate 10
Hostname(config-rate-policy)#downstream average-rate 10 burst-rate 10
Hostname(config)# service-policy user-policy
Hostname(config-service-policy)# rate-policy user-rate apply

```

**Verification** Run the **show running** command to display the speed-limit policy rule.

**Prompt** N/A

**Platform**

## 1.8 service-policy

Use this command to enter user policy configuration mode.

**service-policy** *service-name*

Use this command to apply the specified speed-limit policy.

**rate-policy** *rate-name* **apply**

### Parameter Description

| Parameter           | Description                                              |
|---------------------|----------------------------------------------------------|
| <i>service-name</i> | Indicates the name of the user policy.                   |
| <i>rate-name</i>    | Indicates the name of the speed-limit policy to be used. |

|                               |                                                                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                                                                                                                                            |
| <b>Level</b>                  | 14                                                                                                                                                                                                                                                                                                   |
| <b>Usage Guide</b>            | The name of the speed-limit policy to be used should be configured first.                                                                                                                                                                                                                            |
| <b>Configuration Examples</b> | The following example configures the speed-limit policy to be used and specifies the policy name.                                                                                                                                                                                                    |
| <b>Examples</b>               | <pre> Hostname(config)# rate-policy user-rate Ruijie (config-rate-policy)#upstream average-rate 10 burst-rate 10 Ruijie (config-rate-policy)#downstream average-rate 10 burst-rate 10 Ruijie (config)# service-policy user-policy Ruijie (config-service-policy)# rate-policy user-rate apply </pre> |
| <b>Verification</b>           | Run the <b>show running</b> command to display the user policy configuration.                                                                                                                                                                                                                        |
| <b>Prompt</b>                 | N/A                                                                                                                                                                                                                                                                                                  |
| <b>Platform</b>               | N/A                                                                                                                                                                                                                                                                                                  |

## 1.9 upstream average-rate burst-rate

Use this command to configure the upstream traffic average and burst threshold. Use this command to remove the configuration.

**upstream average-rate** *avg-threshold* **burst-rate** *burst-threshold*  
**no upstream**

| Parameter Description | Parameter              | Description                                                                         |
|-----------------------|------------------------|-------------------------------------------------------------------------------------|
|                       | <i>avg-threshold</i>   | Indicates the traffic average, in KBps. The value ranges from 8 to 261,120.         |
|                       | <i>burst-threshold</i> | Indicates the traffic burst threshold, in KBps. The value ranges from 8 to 261,120. |

|                               |                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------|
| <b>Defaults</b>               | N/A                                                                                |
| <b>Command Mode</b>           | Speed-limit strategy configuration mode                                            |
| <b>Default Level</b>          | 14                                                                                 |
| <b>Usage Guide</b>            | The burst thresholds of upstream parameters must not be smaller than the average.  |
| <b>Configuration Examples</b> | The following example configures the upstream traffic average and burst threshold. |
| <b>Examples</b>               | <pre> Hostname(config)# rate-policy user-rate </pre>                               |

```
Hostname(config-rate-policy)# upstream average-rate 10 burst-rate 10
```

**Verification** Use the **show running** command to display the speed-limit upstream policy rule.

**Prompt** N/A

**Common Errors** N/A

**Platform** N/A



## WLAN QoS Commands

---

1. WLAN QoS Commands
2. WMM Commands



# 1 WLAN QoS Commands

## 1.1 fair-schedule

Use this command to enable fair scheduling on the wireless AP.

Use the **no** form of this command to disable this function.

**fair-schedule**

**no fair-schedule**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command mode** Fat AP: AP configuration mode

**Usage Guide** N/A

**Configuration Examples**  

```
Hostname(config)# fair-schedule
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 illegal-sta-check

Use these commands to enable anti-proxy detection.

Use the **no** form of these commands to restore the default setting.

**illegal-sta-check ip ttl**

**illegal-sta-check tcp source-ports** [ *port-num* ]

**no illegal-sta-check ip ttl**

**no illegal-sta-check tcp source-ports**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           |             |

|                 |                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------|
| <i>port-num</i> | Sets the maximum number of detection ports, in the range from 1 to 512. The default is 512. |
|-----------------|---------------------------------------------------------------------------------------------|

**Defaults** The anti-proxy detection is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Example** The following example enables anti-proxy detection on ap1 with the TTL policy.

```
Hostname(config)# illegal-sta-check ip ttl
```

The following example enables anti-proxy detection on ap2 with the source-port-detection policy. The default port number is 512.

```
Hostname(config)# illegal-sta-check tcp source-ports
```

**Platform Description** N/A

### 1.3 show dot11 ratelimit

Use this command to display WLAN rate limit information.

```
show dot11 ratelimit { wlan | ap | user }
```

| Parameter Description | Parameter   | Description                                       |
|-----------------------|-------------|---------------------------------------------------|
|                       | <b>wlan</b> | Displays the rate limit information of all WLANs. |
|                       | <b>ap</b>   | Displays the rate limit information of all APs.   |
|                       | <b>user</b> | Displays the rate limit information of all users. |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the rate limit information of all APs.

```
Hostname# show dot11 ratelimit ap
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.4 sta-fair

Use this command to specify the fair scheduling priority for a specified user.

Use the **no** form of this command to restore the default setting.

**sta-fair** *mac-address* **priority** *priority*

**no sta-fair** *mac-address*

| Parameter          | Parameter          | Description                                                  |
|--------------------|--------------------|--------------------------------------------------------------|
| <b>Description</b> | <i>mac-address</i> | Specifies the user's MAC address.                            |
|                    | <i>priority</i>    | Sets the fair scheduling priority, in the range from 1 to 6. |

**Defaults** The default is 1 for all STAs by default.

**Command** Global configuration mode  
**Mode**

**Usage Guide** N/A

**Configuration Example**

```
Hostname(config)# sta-fair abcd.1111.1111 priority 2
```

**Platform** N/A  
**Description**

## 1.5 wlan-qos ap-based

Use this command to configure the upstream and downstream traffic limit of the current AP.

Use the **no** form of this command to restore the default setting.

**wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

**no wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit for of the current AP.

Use the **no** form of this command to restore the default setting.

**wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**

**no wlan-qos ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**

| Parameter Description | Parameter                | Description                                                          |
|-----------------------|--------------------------|----------------------------------------------------------------------|
|                       | <b>per-user-limit</b>    | Limit for each user on the AP.                                       |
|                       | <b>total-user-limit</b>  | Limit for the entire AP.                                             |
|                       | <b>down-streams</b>      | Total downstream traffic limit of the AP.                            |
|                       | <b>up-streams</b>        | Total upstream traffic limit of the AP.                              |
|                       | <b>intelligent</b>       | Whether to enable intelligent total-user-limit.                      |
|                       | <i>average-data-rate</i> | Average rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps. |
|                       | <i>burst-data-rate</i>   | Burst rate limit, ranging from 8 to 261,120 in the unit of 8 Kbps.   |

**Defaults** These functions are disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples**  
 Hostname(config)#wlan-qos ap-based per-user-limit down-streams average-data-rate 2000  
 burst-data-rate 5000

| Related Commands | Command                                                                                                                                                                                                                                                     | Description                                                              |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
|                  | <b>wlan-qos netuser</b> <i>mac-address</i> { <b>inbound</b>   <b>outbound</b> } <b>average-data-rate</b> <i>average-data-rate</i> <b>burst-data-rate</b> <i>burst-data-rate</i>                                                                             | Configures the Client-based in-band and out-of-band traffic rate limits. |
|                  | <b>wlan-qos wlan-based</b> { <i>wlan-id</i>   <i>ssid</i> } { <b>per-user-limit</b>   <b>total-user-limit</b> } { <b>down-streams</b>   <b>up-streams</b> } <b>average-data-rate</b> <i>average-data-rate</i> <b>burst-data-rate</b> <i>burst-data-rate</i> | Configures the WLAN-based in-band and out-of-band traffic rate limits.   |

**Platform Description**

## 1.6 wlan-qos netuser

Use this command to configure the in-band and out-of-band traffic limits for a specified user in the current WLAN.

Use the **no** form of this command to restore the default setting.

**wlan-qos netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

**no wlan-qos netuser** *mac-address* { **inbound** | **outbound** }

| Parameter Description | Parameter                | Description                                                        |
|-----------------------|--------------------------|--------------------------------------------------------------------|
|                       | <i>mac-address</i>       | User's MAC address to be set.                                      |
|                       | <b>inbound</b>           | User's in-band traffic limit.                                      |
|                       | <b>outbound</b>          | User's out-of-band traffic limit.                                  |
|                       | <i>average-data-rate</i> | Average rate limit, ranging from 8 to 261120 in the unit of 8Kbps. |
|                       | <i>burst-data-rate</i>   | Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps.   |

**Defaults** No traffic limit is set by default.

**Command mode** Global configuration mode

N/A

**Usage Guide**

**Configuration Examples** `Hostname(config)#wlan-qos netuser abcd.1111.1111 inbound average-data-rate 2000 burst-data-rate 5000`

| Related Commands | Command                                                                                                                                                                                                                                                     | Description                                                            |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
|                  | <b>wlan-qos wlan-based</b> { <i>wlan-id</i>   <i>ssid</i> } { <b>per-user-limit</b>   <b>total-user-limit</b> } { <b>down-streams</b>   <b>up-streams</b> } <b>average-data-rate</b> <i>average-data-rate</i> <b>burst-data-rate</b> <i>burst-data-rate</i> | Configures the WLAN-based in-band and out-of-band traffic rate limits. |
|                  | <b>wlan-qos ap-based</b> { <b>per-user-limit</b>   <b>total-user-limit</b> } { <b>down-streams</b>   <b>up-streams</b> } <b>average-data-rate</b> <i>average-data-rate</i> <b>burst-data-rate</b> <i>burst-data-rate</i>                                    | Configures the AP-based in-band and out-of-band traffic rate limits.   |

**Platform Description**

## 1.7 wlan-qos wlan-based

Use this command to configure the upstream and downstream traffic limit of the current WLAN.

Use the **no** form of this command to restore the default setting.

**wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

**no wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

Use this command to configure the intelligent total-user-limit of the current WLAN. Use the **no** form of this command to restore the default setting.

```
wlan-qos wlan-based { wlan-id | ssid } total-user-limit { down-streams | up-streams }
intelligent
no wlan-qos wlan-based { wlan-id | ssid } total-user-limit { down-streams | up-streams }
intelligent
```

| Parameter Description | Parameter                | Description                                                      |
|-----------------------|--------------------------|------------------------------------------------------------------|
|                       | <i>wlan-id</i>           | WLAN ID.                                                         |
|                       | <i>ssid</i>              | SSID configured by the WLAN.                                     |
|                       | <b>per-user-limit</b>    | Limit for each user on the WLAN.                                 |
|                       | <b>total-user-limit</b>  | Limit for the entire WLAN.                                       |
|                       | <b>down-streams</b>      | Total downstream traffic limit of the WLAN.                      |
|                       | <b>up-streams</b>        | Total upstream traffic limit of the WLAN.                        |
|                       | <b>intelligent</b>       | Whether to enable intelligent total-user-limit.                  |
|                       | <i>average-data-rate</i> | Average rate limit, ranging from                                 |
|                       | <i>burst-data-rate</i>   | Burst rate limit, ranging from 8 to 261120 in the unit of 8Kbps. |

**Defaults** The traffic limit and intelligent total-user-limit are disabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** `Hostname(config)# wlan-qos wlan-based 2 total-user-limit down-streams intelligent`

| Related Commands | Command                                                                                                                                                                        | Description                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
|                  | <b>wlan-qos ap-based { per-user-limit   total-user-limit } { down-streams   up-streams } average-data-rate <i>average-data-rate</i> burst-data-rate <i>burst-data-rate</i></b> | Configures the AP-based in-band and out-of-band traffic rate limits.     |
|                  | <b>netuser mac-address { inbound   outbound } average-data-rate <i>average-data-rate</i> burst-data-rate <i>burst-data-rate</i></b>                                            | Configures the Client-based in-band and out-of-band traffic rate limits. |

**Platform Description**

# 1 WMM Commands

## 1.1 wlan-qos map-table import export

Use this command to configure packet priority mapping for the current WLAN.

Use the **no** form of this command to restore the default setting.

**wlan-qos map-table** { dot11e -dscp | dscp-dot11e } **import** *import-tag-value* **export** *export-tag-value*

**no wlan-qos map-table** { dot11e-dscp | dscp-dot11e } **import** *import-tag-value*

**Parameter Description**

| Parameter                             | Description                                                                                                                                                                                                                                                                       |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dot11e-dscp</b>                    | Sets priority mapping from dot11e to internal DSCP.                                                                                                                                                                                                                               |
| <b>dscp-dot11e</b>                    | Sets priority mapping from DSCP to dot11e.                                                                                                                                                                                                                                        |
| <b>import</b> <i>import-tag-value</i> | Sets priority of the incoming original packet.<br>WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7.<br>DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0. |
| <b>export</b> <i>export-tag-value</i> | Sets priority of the outgoing packet.<br>WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7.<br>DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.          |

**Defaults**

DSCP-to-dot11e Mapping Table

| DSCP  | 802.11e |
|-------|---------|
| 0~7   | 0       |
| 16~23 | 1       |
| 24~31 | 2       |
| 8~15  | 3       |
| 32~39 | 4       |
| 40~47 | 5       |
| 48~55 | 6       |
| 56~63 | 7       |

dot11e-to-DSCP Mapping Table

| 802.11e | DSCP |
|---------|------|
| 0       | 0    |
| 3       | 8    |
| 1       | 16   |
| 2       | 24   |
| 4       | 32   |

|   |    |
|---|----|
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

**Command** WLAN configuration mode  
**Mode**

**Usage Guide** This command is a mapping command for non-interworking versions.  
 The configuration takes effect after the WMM service is enabled.

**Configuration Examples** The following example sets priority mapping from DSCP to dot11e. The priority of the incoming original packet is 1 and that of the outgoing packet is 10.

```

Hostname# configure terminal
Hostname(config)# dot11 wlan 1
Hostname(dot11-wlan-config)# wlan-qos map-table dot11e-dscp import 1
export 10
    
```

**Platform** N/A  
**Description**

## 1.2 wmm dot1p enable

Use this command to enable 802.11p QoS mapping policy mechanism.

Use the **no** form of this command to restore the default setting.

**wmm dot1p enable**

**no wmm dot1p enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command** Dot11radio interface configuration mode.  
**Mode**

**Usage Guide** This command is a mapping command for non-interworking versions.  
 The configuration takes effect after the WMM service is enabled.

**Configuration Examples** The following example enables 802.11p QoS mapping policy mechanism for radio 1 on the AP.

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm dot1p enable
    
```



**Platform**  
**Description** N/A

### 1.3 wmm dot1p policy 1q

Use this command to configure how to apply the 802.11p QoS mapping policy mechanism for the AP. Use the **no** form of this command to restore the default setting.

**wmm dot1p policy 1q** *1q-policy-value*

**no wmm dot1p policy**

| Parameter Description | Parameter                        | Description                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>1q</b> <i>1q-policy-value</i> | Applies the 802.11p QoS mapping policy mechanism, in the range from 0 to 1. The default is 0.<br>Q=1: AP tags the priority domain of 802.1Q according to 802.1p.<br>Q=0: AP tags the priority domain of 802.1Q according to the user priority in the <b>Qos Control</b> field of IEEE 802.11 headers. Apply "Q=1" method when there is no <b>QoS Control</b> field. |
|                       | <b>no</b>                        | Restore the default setting.                                                                                                                                                                                                                                                                                                                                        |

**Defaults** The default is 0.

**Command** Dot11radio interface configuration mode.

**Mode**

**Usage Guide** This command is a mapping command for non-interworking versions.  
The configuration takes effect after the WMM service is enabled.  
The configuration is valid only when the 802.11p QoS mechanism is enabled.

**Configuration** The following example tags the priority domain of 802.1Q for radio 1 on the AP.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm dot1p policy 1q 1

```

**Platform**  
**Description** N/A

### 1.4 wmm dot1p tag

Use this command to configure 802.1p priority.

Use the **no** form of this command to restore the default setting.

**wmm dot1p tag** *tag-value* { **back-ground** | **best-effort** | **video** | **voice** }

**no wmm dot1p tag** { **back-ground** | **best-effort** | **video** | **voice** }

| Parameter Description | Parameter                   | Description                                         |
|-----------------------|-----------------------------|-----------------------------------------------------|
|                       | <b>tag</b> <i>tag-value</i> | Sets the 802.1p priority, in the range from 0 to 7. |
|                       | <b>back-ground</b>          | Sets the back-ground queue.                         |
|                       | <b>best-effort</b>          | Sets the best-effort queue.                         |
|                       | <b>video</b>                | Sets the video queue.                               |
|                       | <b>voice</b>                | Sets the voice queue.                               |
|                       | <b>no</b>                   | Restore the default setting.                        |

**Defaults** The default **best-effort** is 0; the default **back-ground** is 2; the default **video** is 4; the default **voice** is 6.

**Command Mode** Dot11radio interface configuration mode.

**Usage Guide** This command is a mapping command for non-interworking versions.  
 The configuration takes effect after the WMM service is enabled.  
 The configuration is valid only when the 802.11p QoS mechanism is enabled.

**Configuration Examples** The following example sets 802.1p priority to 5 for radio 1 on the AP.

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm dot1p tag 5 voice
    
```

**Platform Description** N/A

## 1.5 wmm dscp enable

Use this command to enable DSCP QoS mapping policy mechanism.  
 Use the **no** form of this command to restore the default setting.

**wmm dscp enable**  
**no wmm dscp enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | -         | -           |

**Defaults** This function is disabled by default.

**Command Mode** Dot11radio interface configuration mode.

**Usage Guide** This command is a mapping command for non-interworking versions.

The configuration takes effect after the WMM service is enabled.

**Configuration** The following example enables DSCP QoS mapping policy mechanism for radio 1 on the AP.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm dscp enable
    
```

**Platform**

N/A

**Description**

## 1.6 wmm dscp policy outer-tunnel inner-tunnel

Use this command to configure how to apply the DSCP QoS mapping policy mechanism for the AP.

Use the **no** form of this command to restore the default setting.

**wmm dscp policy outer-tunnel** *outer-tunnel-value* **inner-tunnel** *inner-tunnel-value*

**no wmm dscp policy**

**Parameter Description**

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>outer-tunnel-value</i> | <p>Configures how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header, in the range from 0 to 1. The default is 0.</p> <p>In the centralized forwarding mode:</p> <p>O=1: AP sets DSCP domain for the tunnel header according to pushed configuration policy;</p> <p>O=0: AP sets DSCP domain for the tunnel header according to inner tunnel packets. If inner tunnel packets are encrypted or non-IPv4/IPv6, the "O=1" method will be applied.</p> <p>In the local forwarding mode:</p> <p>O=1: invalid value;</p> <p>O=0: invalid value.</p>                                                                           |
| <i>inner-tunnel-value</i> | <p>Configures how to apply the DSCP QoS mapping policy mechanism for the inner tunnel header, in the range from 0 to 1. The default is 0.</p> <p>In the centralized forwarding mode:</p> <p>AP sets DSCP domain for the tunnel header according to inner tunnel packets; If inner tunnel packets are encrypted or non-IPv4/IPv6, the "I=1" method will be applied.</p> <p>I=0: AP cannot modify the DSCP domain of user packets.</p> <p>In the local forwarding mode:</p> <p>I=1: AP configures the DSCP domain for user packets according to the pushed configuration policy.</p> <p>I=0: AP cannot modify the DSCP domain of user packets.</p> |

**Defaults**

The default is 0.

|                               |                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command</b>                | Dot11radio interface configuration mode.                                                                                                                                                                                                                                                                               |
| <b>Mode</b>                   |                                                                                                                                                                                                                                                                                                                        |
| <b>Usage Guide</b>            | <p>This command is a mapping command for non-interworking versions.</p> <p>The configuration takes effect after the WMM service is enabled.</p> <p>The configuration is valid only when the DSCP QoS mechanism is enabled.</p>                                                                                         |
| <b>Configuration Examples</b> | <p>The following example sets both outer and inner tunnel headers to 0 for DSCP mapping mechanism of radio 1 on the AP.</p> <pre> Hostname# configure terminal Hostname(config)# interface dot11radio 1/0 Hostname(config-if-Dot11radio 1/0)# wmm dscp policy outer-tunnel 0 inner-tunnel 0                     </pre> |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                                                                                                                    |

## 1.7 wmm dscp tag

Use this command to configure the DSCP identification.

Use the **no** form of this command to restore the default setting.

**wmm dscp tag tag-value { back-ground | best-effort | video | voice }**

**no wmm dscp tag { back-ground | best-effort | video | voice }**

| Parameter Description | Parameter          | Description                                        |
|-----------------------|--------------------|----------------------------------------------------|
|                       | <i>tag-value</i>   | Sets the DSCP priority, in the range from 0 to 63. |
|                       | <b>back-ground</b> | Sets the back-ground queue.                        |
|                       | <b>best-effort</b> | Sets the best-effort queue.                        |
|                       | <b>video</b>       | Sets the video queue.                              |
|                       | <b>voice</b>       | Sets the voice queue.                              |

**Defaults** The default **best-effort** is 0; the default **back-ground** is 16; the default **video** is 32; the default **voice** is 48.

|                               |                                                                                                                                                                                                                              |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command</b>                | Dot11radio interface configuration mode.                                                                                                                                                                                     |
| <b>Mode</b>                   |                                                                                                                                                                                                                              |
| <b>Usage Guide</b>            | <p>This command is a mapping command for non-interworking versions.</p> <p>The configuration takes effect after the WMM service is enabled.</p> <p>DSCP identification is valid only when the DSCP mechanism is enabled.</p> |
| <b>Configuration Examples</b> | <p>The following example sets the DSCP identification to 5 for voice queue of radio 1 on the AP.</p> <pre> Hostname# configure terminal Hostname(config)# interface dot11radio 1/0                     </pre>                |

```
Hostname(config-if-Dot11radio 1/0)# wmm dscp tag 5 voice
```

**Platform**  
**Description**

N/A

## 1.8 wmm edca-client

Use this command to configure the EDCA parameters for the client.

Use the **no** form of this command to restore the default setting.

**wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } [ { **aifsn** *aifsn-value* **cwmin** *cwmin-value* **cwmax** *cwmax-value* **txop** *txop-value* } | **length** *queue-length* ]

**no wmm edca-client** { **back-ground** | **best-effort** | **video** | **voice** } [ **length** ]

| Parameter Description | Parameter                         | Description                                                                  |
|-----------------------|-----------------------------------|------------------------------------------------------------------------------|
|                       | <b>back-ground</b>                | Sets the back-ground queue.                                                  |
|                       | <b>best-effort</b>                | Sets the best-effort queue.                                                  |
|                       | <b>video</b>                      | Sets the video queue.                                                        |
|                       | <b>voice</b>                      | Sets the voice queue.                                                        |
|                       | <b>aifsn</b> <i>aifsn-value</i>   | Sets the <b>aifsn</b> value, in the range from 1 to15.                       |
|                       | <b>cwmin</b> <i>cwmin-value</i>   | Sets the <b>cwmin</b> value, in the range from 0 to 15.                      |
|                       | <b>cwmax</b> <i>cwmax-value</i>   | Sets the <b>cwmax</b> value, in the range from 0 to 15.                      |
|                       | <b>txop</b> <i>txop-value</i>     | Sets the <b>txop</b> value, in the range from 0 to 255 in the unit of 32 μs. |
|                       | <b>length</b> <i>queue-length</i> | Sets the AC queue length in the range from 1 to 255. The default is 255.     |

| Defaults | AC                 | aifs | cwmin | cwmax | txop |
|----------|--------------------|------|-------|-------|------|
|          | <b>back-ground</b> | 7    | 4     | 10    | 0    |
|          | <b>best-effort</b> | 3    | 4     | 10    | 0    |
|          | <b>video</b>       | 2    | 3     | 4     | 94   |
|          | <b>voice</b>       | 2    | 2     | 3     | 47   |

**Command** Dot11radio interface configuration mode.

**Mode**

**Usage Guide** The configuration takes effect after the WMM service is enabled.

The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

**Configuration Examples** The following example configures **asfsn** to 2, **cwmin** to 2, **cwmax** to 3 and **txop** to 50 for the voice queue of radio 1 on the AP.

```
Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
```

```
Hostname(config-if-Dot11radio 1/0)# wmm edca-client voice aifsn 2 cwmin 2
cwmax 3 txop 50
```

**Platform** N/A  
**Description**

## 1.9 wmm edca-radio

Use this command to configure the EDCA parameters for the AP.

Use the **no** form of this command to restore the default setting.

**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } [ { **aifsn** *aifsn-value* **cwmin** *cwmin-value* **cwmax** *cwmax-value* **txop** *txop-value* } | **noack** ]

**no wmm edca-radio** { **back-groud** | **best-effort** | **video** | **voice** } [ **noack** ]

**Parameter**  
**Description**

| Parameter                       | Description                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------|
| <b>back-ground</b>              | Sets the back-ground queue.                                                            |
| <b>best-effort</b>              | Sets the best-effort queue.                                                            |
| <b>video</b>                    | Sets the video queue.                                                                  |
| <b>voice</b>                    | Sets the voice queue.                                                                  |
| <b>aifsn</b> <i>aifsn-value</i> | Sets the <b>aifsn</b> value, in the range from 1 to 15.                                |
| <b>cwmin</b> <i>cwmin-value</i> | Sets the <b>cwmin</b> value, in the range from 0 to 15.                                |
| <b>cwmax</b> <i>cwmax-value</i> | Sets the <b>cwmax</b> value, in the range from 0 to 15.                                |
| <b>txop</b> <i>txop-value</i>   | Sets the <b>txop</b> value, in the range from 0 to 255 in the unit of 32 μs.           |
| <b>noack</b>                    | Indicates that the no ack policy is enabled. The no ack policy is disabled by default. |

**Defaults**

| AC                 | aifs | cwmin | cwmax | txop |
|--------------------|------|-------|-------|------|
| <b>back-ground</b> | 7    | 4     | 10    | 0    |
| <b>best-effort</b> | 3    | 4     | 6     | 0    |
| <b>video</b>       | 1    | 3     | 4     | 94   |
| <b>voice</b>       | 1    | 2     | 3     | 47   |

**Command** Dot11radio interface configuration mode.  
**Mode**

**Usage Guide** The configuration takes effect after the WMM service is enabled.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

The **cwmax** value must be greater than the **cwmin** value. Otherwise, a configuration error message is displayed.

**Configuration** The following example sets **aifsn** to 1, **cwmin** to 1, **cwmax** to 3, **txop** to 50 for the voice queue of radio 1 on  
**Examples** the AP.

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm edca-radio voice aifsn 1 cwmin 1
cwmax 3 txop 50
    
```

**Platform** N/A  
**Description**

## 1.10 wmm enable

Use this command to enable the WMM service.  
 Use **no** form of this command to disable the WMM service.

**wmm enable**  
**no wmm enable**

**Parameter**  
**Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command** Dot11radio interface configuration mode.  
**Mode**

**Usage Guide** When the WMM service is disabled, the default priority queue is used for reception and mapping.

**Configuration** The following example enables the WMM service for radio 1 on the AP.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface dot11radio 1/0
Hostname(config-if-Dot11radio 1/0)# wmm enable
    
```

**Platform** N/A  
**Description**



# WLAN Distributed System Commands

---

1. WDS Commands



# 1 WDS Commands

## 1.1 show dot11 wds-bridge-info

Use this command to display WDS bridge configuration.

**show dot11 wds-bridge-info** *interface-name*

| Parameter Description | Parameter             | Description                |
|-----------------------|-----------------------|----------------------------|
|                       | <i>interface-name</i> | Dot11radio interface name. |

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays WDS bridge configuration.

**Examples**

```

Hostname# show dot11 wds-bridge-info 1/0
WDS-MODE: ROOT-BRIDGE
BRIDGE-WLAN:
    Status OK
WlanID 1, SSID ruijie_root, BSSID 32d0.f822.3303

WBI 1/0
NONROOT 00d0.f822.3304

WBI 1/1
NONROOT 00d0.f822.3307
    
```

**Field Description**

| Field       | Description           |
|-------------|-----------------------|
| WDS-MODE    | WDS bridge mode.      |
| BRIDGE-WLAN | WLAN used for bridge. |
| WBI         | WDS bridge link.      |

The following example displays WDS bridge configuration.

```

Hostname# show dot11 wds-bridge-info 1/0
WDS-MODE: ROOT-BRIDGE
BRIDGE-WLAN:
    Status WAITING
    
```

```
Wlanid 1
```

The following example displays WDS bridge configuration.

```
Hostname# show dot11 wds-bridge-info 1/0
WDS-MODE: NONROOT-BRIDGE
MAC: 00d0.f822.3304

WBI 1/0
    ROOT 32d0.f822.3303
```

**Platform**  
**Description** N/A

### 1.2 show wds-mode

Use this command to display the WDS bridge mode configuration on APs.

show wds-mode

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Command**  
**Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the WDS bridge mode configuration on APs.

**Configuration** The following example displays the WDS bridge mode configuration.

**Examples**

```
Hostname# show wds-mode
wds-mode disable.
```

**Platform**  
**Description** This command is supported only on AP devices.

### 1.3 station-role

Use this command to specify AP bridge mode.

Use the **no** form of this command to restore the default setting.

**station-role** { **root-ap** | **root-bridge bridge-wlan** *wlan-id* | **non-root-bridge** }  
**no station-role**

| Parameter Description | Parameter              | Description                                  |
|-----------------------|------------------------|----------------------------------------------|
|                       | <b>root-ap</b>         | Sets the AP working mode as non-bridge mode. |
|                       | <b>non-root-bridge</b> | Sets the AP working mode as non-root bridge. |
|                       | <b>root-bridge</b>     | Sets the AP working mode as root bridge.     |
|                       | <i>wlan-id</i>         | WLAN ID used for root bridge.                |

**Defaults** The default is non-bridge mode.

**Command Mode** Dot11radio interface configuration mode

**Usage Guide** To apply WDS, you must first specify an AP bridge mode. The non-root fit bridge mode is enabled not on ACs but APs.  
 For APs in the root bridge mode, the WLAN ID used for root bridge must be specified. If not, WDS cannot start. Furthermore, the WLAN SSID should not be hidden, or the bridge may fail.  
 It is better to have professional technicians conduct non-root configuration on ACs. If the configuration is incorrect, the non-root bridge will lose connection with the AC.

**Configuration Examples** The following example specifies the root bridge mode on the AP.

```
Hostname(config-if-Dot11radio 1/0)# station-role root-bridge
bridge-wlan 1
```

The following example specifies the non-root bridge mode on the AP.

```
Hostname(config-if-Dot11radio 1/0)# station-role non-root-bridge
```

| Related Commands | Command                                      | Description                                    |
|------------------|----------------------------------------------|------------------------------------------------|
|                  | <b>parent mac-address</b> <i>mac-address</i> | Configures the MAC address of the parent node. |

**Platform Description** N/A

## 1.4 wds ctrl eth

Use this command to enable Ethernet port control (only for non-root bridge mode).


**wds ctrl eth**  
**no wds ctrl eth**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This function is configured on APs for non-root fat bridge and on ACs for non-root fit bridge.

 Use this command carefully. Once it is configured, Ethernet ports will be disconnected if the bridging fails. Thereby, ACs will lose control of APs.

**Configuration** The following configuration enables Ethernet port control on the AP.

**Examples** `Hostname(config)#wds ctrl eth`

The following configuration enables Ethernet port control on the AC.

`Hostname(config-ap)#wds ctrl eth`

**Related Commands**

| Command                             | Description                                |
|-------------------------------------|--------------------------------------------|
| <code>show running-config</code>    | Displays the running configuration.        |
| <code>show ap-config running</code> | Displays the running configuration on APs. |

**Platform** N/A

**Description**

## 1.5 wds pre-config

Use this command to create or delete non-root pre-configuration.

`wds pre-config { create | delete }`




**Parameter Description**

| Parameter           | Description                                |
|---------------------|--------------------------------------------|
| <code>create</code> | Creates pre-configuration only on fat APs. |
| <code>delete</code> | Deletes pre-configuration.                 |

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** This command is pre-configuration for non-root fat APs working in the non-root fit mode.

-  The **wds pre-config create** command is configured only on fat APs. It specifies the current non-root configuration of the fat AP as the pre-configuration of the non-root fit mode. Then, it restores the fat AP's default setting.
-  Before the non-root fit AP works in the non-root fit mode, it must get pre-configured.
-  When the WDS bridge mode is disabled, use the **wds pre-config delete** command to delete configuration files on the non-root end.

**Configuration** The following example pre-configures ruijie-root as its access root end on the fat AP.

**Examples**

```

Hostname(config-if-Dot11radio 1/0)# station-role non-root-bridge
Hostname(config-if-Dot11radio 1/0)# parent ssid ruijie-root
Hostname(config-if-Dot11radio 1/0)# wds pre-config create
Hostname(config-if-Dot11radio 1/0)# exit
Hostname(config)# exit
Hostname# ap-mode fit
    
```

The following example removes WDS non-root pre-configuration on the AP.

```

Hostname(config-if-Dot11radio 1/0)# wds pre-config delete
    
```

**Related Commands** N/A

**Platform Description** N/A

## 1.6 wds-mode enable

Use this command to enable WDS bridge mode (only for WDS bridge-capable AP).

**wds-mode enable**

Use this command to disable WDS bridge mode.

**wds-mode disable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** AP will restart after this command is executed.

**Configuration** The following example enables WDS bridge mode on the AP.

**Examples** `Hostname (config)# wds-mode enable`

**Related  
Commands** N/A

**Platform  
Description** N/A



# WLAN Optimization and Maintenance Commands

---

1. WLOG Commands
2. DATA-PLANE Commands

# 1 WLOG Commands

## 1.1 show wlan diag sta

Use the following command to display STA statistics on an AP:

**show wlan diag sta** [ *sta-mac* *sta-mac* ] [ *number* *number* ]

| Parameter Description | Parameter      | Description                                              |
|-----------------------|----------------|----------------------------------------------------------|
|                       | <i>sta-mac</i> | Specifies the MAC address of an STA.                     |
|                       | <i>number</i>  | Specifies the maximum number of records to be displayed. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** The memory pre-allocation is performed when the WLAN-WLOG function is enabled. If the memory is insufficient, the WLAN-WLOG function cannot be enabled. Memories of all saved information and pre-allocated memories are set free when the WLOG function is disabled.

**Configuration Examples** This example displays STA statistics on an AP.

```

Hostname# show wlan diag sta
sta mac: c83a.35c6.0c72
=====
=====
2012-05-28 19:31:08
wlan id  state      rssi_rt  rs_rate_mcs  tx_frm_cnts  rx_frm_cnts  tx_frm_flow
rx_frm_flow  tx_cnts_error  tx_flow_error  mgmt_cnts  mgmt_flow
-----
-----
1          3          23        80           18           59           4384       5967
0          0           3         381
tx/rxmcs   mcs0, mcs1   mcs2, mcs3   mcs4, mcs5   mcs6, mcs7   mcs8, mcs9
mcs10, mcs11  mcs12, mcs13  mcs14, mcs15
-----
-----
txmcspercent : 0      0      0      0      0      0      0      0
rxmcspercent : 0      0      0      0      0      0      0      0
    
```



```

tx/rxrate      1, 2      5.5, 11 6, 9      12, 18 24, 36 48, 54  --      --
-----
txratepercent: 16      0      0      7      50      27      0      0
rxratepercent: 57      3      0      5      13      22      0      0
    
```

| Field      | Description                                                        |
|------------|--------------------------------------------------------------------|
| sta_record | Specifies STA records.                                             |
| TIME       | Specifies the time when STA records are collected.                 |
| IP Address | Specifies the IP address of an STA whose statistics are collected. |
| Rssi       | Specifies signal strength.                                         |
| Link Rate  | Specifies a connection rate.                                       |
| AP MAC     | Specifies the MAC address of an AP associated with the STA.        |
| SSID       | Specifies the SSID of the WLAN associated with the STA.            |
| RADIO      | Specifies the ID of the radio associated with the STA.             |
| Action     | Specifies the type of STA action records.                          |
| Result     | Specifies the result of STA action records.                        |
| Reason     | Specifies the reason for STA action records.                       |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description**

N/A

## 1.2 wlan diag enable

Use this command to enable the WLAN log (WLOG) . Use the **no** form of this command to disable WLOG.

**wlan diag enable**

**no wlan diag enable**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

The WLOG function is disabled on APs by default.

**Command**

Global configuration mode

**Mode**

**Usage Guide** The memory pre-allocation is performed when the WLAN-WLOG function is enabled. If the memory is insufficient, the WLAN-WLOG function cannot be enabled.

Memories of all saved information and pre-allocated memories are set free when the WLOG function is disabled.

**Configuration** The following example enables and disables the WLOG function.

**Examples**

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#wlan diag enable
Hostname(config)#no wlan diag enable
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description** N/A

# 1 DATA-PLANE Commands

## 1.1 data-plane arp-control enable

Use this command to enable ARP broadcast control.

**data-plane arp-control enable**

Use the **no** form of this command to disable ARP broadcast control.

**no data-plane arp-control enable**

**Parameter Description** N/A

**Defaults** ARP broadcast control is disabled by default.

**Command mode** Global configuration mode

**Usage Guide** -

**Configuration** The following example enables ARP broadcast control.

**Examples**

```

Hostname(config)# data-plane arp-control enable
Hostname(config)#
    
```

**Platform Description** AP

## 1.2 data-plane arp-control vlan trusted-host

Use this command to configure the trusted host for ARP broadcast control.

**data-plane arp-control vlan *vlan-id* trusted-host *ipv4-address***

Use the **no** form of this command to delete the trusted host.

**no data-plane arp-control vlan *vlan-id* trusted-host *ipv4-address***

| Parameter Description | Parameter           | Description                                                                          |
|-----------------------|---------------------|--------------------------------------------------------------------------------------|
|                       | <i>vlan-id</i>      | Specifies a VLAN for ARP broadcast control. The range is from 1 to 4094.             |
|                       | <i>ipv4-address</i> | Specifies the IPv4 address of a trusted host. Up to 64 IPv4 addresses are supported. |

|                      |                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>      | No trusted host is configured for ARP broadcast control.                                                                               |
| <b>Command mode</b>  | Global configuration mode                                                                                                              |
| <b>Usage Guide</b>   | -                                                                                                                                      |
| <b>Configuration</b> | The following example enables ARP broadcast control and configures a trusted host whose IP address is 10.233.1.65.                     |
| <b>Examples</b>      | <pre> Hostname(config)# data-plane arp-control enable Hostname(config)# data-plane arp-control vlan 10 trusted-host 10.233.1.65 </pre> |
| <b>Platform</b>      | AP                                                                                                                                     |
| <b>Description</b>   |                                                                                                                                        |

### 1.3 data-plane close-arp-filter

Configure this function if you want to broadcast ARP packets to the CAPWAP tunnel interface.

**data-plane close-arp-filter { enable | disable }**

Use the **no** form of this command to restore the default setting.

**no data-plane close-arp-filter**

| <b>Parameter Description</b> | Parameter      | Description                                                               |
|------------------------------|----------------|---------------------------------------------------------------------------|
|                              | <b>enable</b>  | Allows ARP packets to be broadcast to the CAPWAP tunnel interface.        |
|                              | <b>disable</b> | Prevents ARP packets from being broadcast to the CAPWAP tunnel interface. |

**Defaults** ARP packets are not broadcast to the CAPWAP tunnel interface by default.

**Command mode** Global configuration mode

**Default Level** c  
15

**Usage Guide** -

**Configuration** Disable ARP broadcast isolation in global configuration mode.

**Examples**

```

Hostname(config)#data-plane close-arp-filter enable

```

**Verification** -

**Notifications** -

**Common** -

**Errors**

**Platform**

**Description** -

### 1.4 data-plane close-mdns-filter

Configure this function to allow mDNS packets to pass through.

**data-plane close-mdns-filter { enable | disable }**

Use the no form of this command to restore the default setting.

**no data-plane close-mdns-filter**

**Parameter Description**

| Parameter      | Description                                                      |
|----------------|------------------------------------------------------------------|
| <b>enable</b>  | Allows mDNS packets to be forwarded to the air interface.        |
| <b>disable</b> | Prevents mDNS packets from being forwarded to the air interface. |

**Defaults**

mDNS packets are not forwarded to the wireless network by default.

**Command mode**

Global configuration mode

**Default Level**

15

**Usage Guide**

-

**Configuration**

Configure the AP to allow mDNS packets to pass through in the global configuration mode.

**Examples**

```
Hostname(config)#data-plane close-mdns-filter enable
```

**Verification**

-

**Notifications**

-

**Common Errors**

-

**Platform**

**Description** -

### 1.5 data-plane close-nd-filter

Configure this function to broadcast ND packets to the CAPWAP tunnel interface.

**data-plane close-nd-filter { enable | disable }**

Use the no form of this command to restore the default setting.

**no data-plane close-nd-filter**

| Parameter Description | Parameter      | Description                                                              |
|-----------------------|----------------|--------------------------------------------------------------------------|
|                       | <b>enable</b>  | Allows ND packets to be broadcast to the CAPWAP tunnel interface.        |
|                       | <b>disable</b> | Prevents ND packets from being broadcast to the CAPWAP tunnel interface. |

**Defaults** ND packets are not broadcast to the CAPWAP tunnel interface by default.

**Command mode** Global configuration mode

**Default Level** 15

**Usage Guide** -

**Configuration** Configure the AP to allow ND packets to pass through in the global configuration mode.

**Examples** `Hostname(config)# data-plane close-nd-filter enable`

**Verification** -

**Notifications** -

**Common Errors** -

**Platform Description** -

## 1.6 data-plane close-ospf-filter

Configure this function to allow OSPF packets to pass through.

**data-plane close-ospf-filter { enable | disable }**

Use the no form of this command to restore the default setting.

**no data-plane close-ospf-filter**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                             |                                                                                                                                                                                                                                               |               |                                                           |                |                                                                  |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------|----------------|------------------------------------------------------------------|
| <b>Description</b>          |                                                                                                                                                                                                                                               |               |                                                           |                |                                                                  |
|                             | <table border="1"> <tr> <td><b>enable</b></td> <td>Allows OSPF packets to be forwarded to the air interface.</td> </tr> <tr> <td><b>disable</b></td> <td>Prevents OSPF packets from being forwarded to the air interface.</td> </tr> </table> | <b>enable</b> | Allows OSPF packets to be forwarded to the air interface. | <b>disable</b> | Prevents OSPF packets from being forwarded to the air interface. |
| <b>enable</b>               | Allows OSPF packets to be forwarded to the air interface.                                                                                                                                                                                     |               |                                                           |                |                                                                  |
| <b>disable</b>              | Prevents OSPF packets from being forwarded to the air interface.                                                                                                                                                                              |               |                                                           |                |                                                                  |
| <b>Defaults</b>             | OSPF packets are not forwarded to the wireless network by default.                                                                                                                                                                            |               |                                                           |                |                                                                  |
| <b>Command mode</b>         | Global configuration mode                                                                                                                                                                                                                     |               |                                                           |                |                                                                  |
| <b>Default Level</b>        | 15                                                                                                                                                                                                                                            |               |                                                           |                |                                                                  |
| <b>Usage Guide</b>          | -                                                                                                                                                                                                                                             |               |                                                           |                |                                                                  |
| <b>Configuration</b>        | Configure the AP to allow OSPF packets to pass through in the global configuration mode.                                                                                                                                                      |               |                                                           |                |                                                                  |
| <b>Examples</b>             | <pre>Hostname(config)#data-plane close-ospf-filter enable</pre>                                                                                                                                                                               |               |                                                           |                |                                                                  |
| <b>Verification</b>         | -                                                                                                                                                                                                                                             |               |                                                           |                |                                                                  |
| <b>Notifications</b>        | -                                                                                                                                                                                                                                             |               |                                                           |                |                                                                  |
| <b>Common Errors</b>        | -                                                                                                                                                                                                                                             |               |                                                           |                |                                                                  |
| <b>Platform Description</b> | -                                                                                                                                                                                                                                             |               |                                                           |                |                                                                  |

## 1.7 data-plane close-ssdp-filter

Configure this function to allow SSDP packets to pass through.

**data-plane close-ssdp-filter { enable | disable }**

Use the no form of this command to restore the default setting.

**no data-plane close-ssdp-filter**

| <b>Parameter Description</b> |                                                                                                                                                                                                                                                                                                                                    |           |             |               |                                                           |                |                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|---------------|-----------------------------------------------------------|----------------|------------------------------------------------------------------|
|                              | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>enable</b></td> <td>Allows SSDP packets to be forwarded to the air interface.</td> </tr> <tr> <td><b>disable</b></td> <td>Prevents SSDP packets from being forwarded to the air interface.</td> </tr> </tbody> </table> | Parameter | Description | <b>enable</b> | Allows SSDP packets to be forwarded to the air interface. | <b>disable</b> | Prevents SSDP packets from being forwarded to the air interface. |
| Parameter                    | Description                                                                                                                                                                                                                                                                                                                        |           |             |               |                                                           |                |                                                                  |
| <b>enable</b>                | Allows SSDP packets to be forwarded to the air interface.                                                                                                                                                                                                                                                                          |           |             |               |                                                           |                |                                                                  |
| <b>disable</b>               | Prevents SSDP packets from being forwarded to the air interface.                                                                                                                                                                                                                                                                   |           |             |               |                                                           |                |                                                                  |

**Defaults** SSDP packets are not forwarded to the wireless network by default.

**Command** Global configuration mode

**mode****Default Level** 15**Usage Guide** -**Configuration** Configure the AP to allow SSDP packets to pass through in the global configuration mode.**Examples**

```
Hostname(config)#data-plane close-ssdp-filter enable
```

**Verification** -**Notifications** -**Common Errors** -**Platform** -**Description**

## 1.8 data-plane close-vrrp-filter

Configure this function to allow OSPF packets to pass through.

**data-plane close-vrrp-filter { enable | disable }**

Use the no form of this command to restore the default setting.

**no data-plane close-vrrp-filter**

| Parameter Description | Parameter      | Description                                                      |
|-----------------------|----------------|------------------------------------------------------------------|
|                       | <b>enable</b>  | Allows VRRP packets to be forwarded to the air interface.        |
|                       | <b>disable</b> | Prevents VRRP packets from being forwarded to the air interface. |

**Defaults** VRRP packets are not forwarded to the wireless network by default.**Command mode** Global configuration mode**Default Level** 15**Usage Guide** -**Configuration** Configure the AP to allow VRRP packets to pass through in the global configuration mode.**Examples**

```
Hostname(config)#data-plane close-vrrp-filter enable
```



|                      |   |
|----------------------|---|
| <b>Verification</b>  | - |
| <b>Notifications</b> | - |
| <b>Common Errors</b> | - |
| <b>Platform</b>      | - |
| <b>Description</b>   | - |

## 1.9 data-plane queue-weight

Use this command to configure the queue weight for different packets.

**data-plane queue-weight** *unicast-packet-weight* *multicast-packet-weight* *broadcast-packet-weight* *unknown-multicast-packet-weight* *unknown-unicast-packet-weight*

Use the **no** form of this command to restore the default setting.

**no data-plane queue-weight**

| Parameter Description | Parameter                              | Description                                                                                                 |
|-----------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------|
|                       | <i>unicast-packet-weight</i>           | Sets the forwarding weight of unicast packets. The range is from 1 to 100. The default value is 16.         |
|                       | <i>multicast-packet-weight</i>         | Sets the forwarding weight of multicast packets. The range is from 1 to 50. The default value is 4.         |
|                       | <i>broadcast-packet-weight</i>         | Sets the forwarding weight of broadcast packets. The range is from 1 to 50. The default value is 2.         |
|                       | <i>unknown-multicast-packet-weight</i> | Sets the forwarding weight of unknown multicast packets. The range is from 1 to 25. The default value is 1. |
|                       | <i>unknown-unicast-packet-weight</i>   | Sets the forwarding weight of unknown unicast packets. The range is from 1 to 25. The default value is 1.   |

**Defaults** The queue weight configuration for different packets is enabled by default.

**Command mode** Global configuration mode

**Usage Guide** -

**Configuration Examples** The following example configures the queue weight for different packets.

```
Hostname(config)# data-plane queue-weight 100 50 50 25 25
```

**Platform Description** AP

## 1.10 data-plane token

Use this command to configure the update interval and token rate of token bucket.

**data-plane token** *token-interval token-base-rate*

Use the **no** form of this command to restore the default setting.

**no data-plane token**

| Parameter Description | Parameter              | Description                                                                                                 |
|-----------------------|------------------------|-------------------------------------------------------------------------------------------------------------|
|                       | <i>token-interval</i>  | Sets the update interval of the token bucket. The default interval is 1. The value ranges from 1 to 10,000. |
|                       | <i>token-base-rate</i> | Sets the token rate of the token bucket. The value ranges from 1 to 1,000,000. The default value is 5.      |

**Defaults** The default update interval is 10 milliseconds.  
The default token rate of the token bucket is 5.

**Command mode** Global configuration mode

**Usage Guide** -

**Configuration** The following example sets the token rate of the token bucket to 20 at an interval of 10 milliseconds.

**Examples**

```
Hostname(config)# data-plane token 1 20
```

**Platform** AP  
**Description**

## 1.11 data-plane wireless-broadcast

Use this command to enable or disable the wireless broadcast function.

**data-plane wireless-broadcast** { **enable** | **disable** }

Use the **no** form of this command to restore the default setting.

**no data-plane wireless-broadcast**

| Parameter Description | Parameter      | Description                               |
|-----------------------|----------------|-------------------------------------------|
|                       | <b>enable</b>  | Enables the wireless broadcast function.  |
|                       | <b>disable</b> | Disables the wireless broadcast function. |

**Defaults** The wireless broadcast function is disabled by default.

**Command** Global configuration mode  
**mode**

**Usage Guide** -

**Configuration** The following example enables the wireless broadcast function.

**Examples** `Hostname(config)# data-plane wireless-broadcast enable`

**Platform**  
**Description** AP



## Security Commands

---

1. ACL Commands
2. ARP Check Commands
3. Gateway-targeted ARP Spoofing Prevention Commands
4. Global IP-MAC Address Binding Commands
5. IP Source Guard Commands
6. CPP Commands
7. NFPP Commands
8. Password Policies Commands
9. SSH Commands

# 1 ACL Commands

## 1.1 access-list

Use this command to create an access list to filter data packets.

- Create an IP standard ACL and add a rule.

```
access-list acl-id { deny | permit } { source-ip-address source-ip-wildcard | any | host
source-ip-address } [ time-range time-range-name ]
```

- Create an IP extended ACL and add a rule.

```
access-list acl-id { deny | permit } protocol { source source-wildcard | any | host source } [ lt port |
eq port | gt port | neq port | range lower upper ] { destination destination-wildcard | any | host
destination } [ lt port | eq port | gt port | neq port | range lower upper ] [ time-range
time-range-name ]
```

- Create a MAC extended ACL and add a rule.

```
access-list acl-id { deny | permit } { source-mac-address source-mac-mask | any | host
source-mac-address } { destination-mac-address destination-mac-mask | any | host
destination-mac-address } [ ethernet-type ] [ cos [ cos ] [ inner cos ] ]
```

- Create an expert extended ACL and add a rule.

```
access-list acl-id { deny | permit } [ protocol | [ ethernet-type ] [ cos [ cos ] [ inner cos ] ] ] [ VID [ vid ]
[ inner vid ] ] { source source-wildcard | any | host source } { source-mac-address
source-mac-mask | any | host source-mac-address } [ lt port | eq port | gt port | neq port | range
lower upper ] { destination destination-wildcard | any | host destination } { any | host
destination-mac-address } [ lt port | eq port | gt port | neq port | range lower upper ] [ time-range
time-range-name ]
```

- When you select the Ethernet-type field or cos field:

```
access-list acl-id { deny | permit } { ethernet-type | cos [ cos ] [ inner cos ] } [ VID [ vid ] [ inner vid ] ]
{ source source-wildcard | any | host source } { source-mac-address source-mac-mask | any | host
source-mac-address } { destination destination-wildcard | any | host destination } { any | host
destination-mac-address } [ time-range time-range-name ]
```

- When you select the protocol field:

```
access-list acl-id { deny | permit } protocol [ VID [ vid ] [ inner vid ] ] { source source-wildcard | any |
host source } { source-mac-address source-mac-mask | any | host source-mac-address } [ lt port |
eq port | gt port | neq port | range lower upper ] { destination destination-wildcard | any | host
destination } { any | host destination-mac-address } [ lt port | eq port | gt port | neq port | range lower
upper ] [ time-range time-range-name ]
```

- Extended expert ACLs of some important protocols:

**Internet Control Message Protocol (ICMP)**

```
access-list acl-id { deny | permit } icmp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | any |
host source } { source-mac-address source-mac-mask | any | host source-mac-address }
{ destination destination-wildcard | any | host destination } { any | host destination-mac-address }
[ icmp-type ] [ [ icmp-type [ icmp-code ] ] | [ icmp-message ] ] [ time-range time-range-name ]
```

**Transmission Control Protocol (TCP)**

```
access-list acl-id { deny | permit } tcp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | any | host
source } { source-mac-address source-mac-mask | any | host source-mac-address } [ lt port | eq port
| gt port | neq port | range lower upper ] { destination destination-wildcard | any | host destination }
{ any | host destination-mac-address } [ lt port | eq port | gt port | neq port | range lower upper ]
[ time-range time-range-name ]
```

**User Datagram Protocol (UDP)**

```
access-list acl-id { deny | permit } udp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | any |
host source } { source-mac-address source-mac-mask | any | host source-mac-address } [ lt port |
eq port | gt port | neq port | range lower upper ] { destination destination-wildcard | any | host
destination } { any | host destination-mac-address } [ lt port | eq port | gt port | neq port | range lower
upper ] [ time-range time-range-name ]
```

Use the **no** form of this command to remove the specified access list.

**no access-list** *acl-id*

**Parameter Description**

| Parameter                   | Description                                                                                                                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl-id</i>               | Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.                                                                                                                            |
| <b>deny</b>                 | If not matched, access is denied.                                                                                                                                                                                                                      |
| <b>permit</b>               | If matched, access is permitted.                                                                                                                                                                                                                       |
| <i>source</i>               | Specify the source IP address (host address or network address).                                                                                                                                                                                       |
| <i>source-wildcard</i>      | Source IP address wildcard mask, which is used to match the source IP addresses of multiple hosts. The wildcard masks can be discontinuous, for example, 0.255.0.32.                                                                                   |
| <i>protocol</i>             | IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately. |
| <i>destination</i>          | Specify the destination IP address (host address or network address).                                                                                                                                                                                  |
| <i>destination-wildcard</i> | Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.                                                                                                                                                              |
| <b>time-range</b>           | Time range of packet filtering                                                                                                                                                                                                                         |
| <i>time-range-name</i>      | Time range name of packet filtering                                                                                                                                                                                                                    |
| <i>icmp-type</i>            | ICMP message type (0 to 255)                                                                                                                                                                                                                           |

|                                            |                                                                                                                                                                              |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>icmp-code</i>                           | ICMP message type code (0 to 255)                                                                                                                                            |
| <i>icmp-message</i>                        | ICMP message type name                                                                                                                                                       |
| <b>host</b> <i>source-mac-address</i>      | Source physical address                                                                                                                                                      |
| <b>host</b> <i>destination-mac-address</i> | Destination physical address                                                                                                                                                 |
| <b>cos</b> <i>cos</i>                      | Matches the priority field value in the outer tag in the L2 packets. The value range is from 0 to 7.                                                                         |
| <b>inner</b> <i>cos</i>                    | Matches the priority field value in the inner tag in the L2 packets. The value range is from 0 to 7.                                                                         |
| <b>VID</b> <i>vid</i>                      | Matches the VLAN ID. The value range is from 1 to 4094.                                                                                                                      |
| <b>inner</b> <i>vid</i>                    | Matches the inner VLAN ID. The value range is from 1 to 4094.                                                                                                                |
| <i>ethernet-type</i>                       | Ethernet protocol type for matching. The value range is from 0x0000 to 0xFFFF. Some important Ethernet protocol type names such as arp, aarp, and IPX are listed separately. |
| <b>lt</b> <i>port match-all</i>            | Matches all the bits of the TCP flag.                                                                                                                                        |
| <b>gt</b> <i>porttcp-flag</i>              | Matches packets with the L4 port ID greater than the specified value. The value range is from 0 to 65535.                                                                    |
| <b>eq</b> <i>port</i>                      | Matches packets with the L4 port ID equal to the specified value. The value range is from 0 to 65535.                                                                        |
| <b>established</b>                         | Matches only the RST or ACK bit in the TCP flag, not the other bits.                                                                                                         |
| <i>lower</i>                               | Lower limit of the L4 port ID range for matching. The value range is from 0 to 65535.                                                                                        |
| <i>upper</i>                               | Upper limit of the L4 port ID range for matching. The value range is from 0 to 65535.                                                                                        |

**Defaults** N/A

**Command** Global configuration mode.

**Mode**

**Usage Guide** To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs:

The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses.

The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses.

The MAC extended ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

The expert extended access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID.

For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: **precedence** *precedence/tos* *tos/fragments/range* *lower upper/time-range* *time-range-name*

The TCP Flag includes part or all of the following:

- urg

- ack
- psh
- rst
- syn
- fin

The packet precedence is as below:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The service types are as below:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect



- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen

- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldp
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff

- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat

- larc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

The UDF headers are as below:

- l2-head
- l3-head
- l4-head
- l5-head

 To remove ACL rules, run the **no { sn | permit | deny }** command in ACL configuration mode.

#### Configuration 1. Example of the standard IP ACL

#### Examples

The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

```
Hostname(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

#### 2. Example of the extended IP ACL

The following extended IP ACL allows the DNS messages and ICMP messages to pass:

```
Hostname(config)# access-list 102 permit tcp any any eq domain log
Hostname(config)# access-list 102 permit udp any any eq domain log
Hostname(config)# access-list 102 permit icmp any any echo log
Hostname(config)# access-list 102 permit icmp any any echo-reply
```

#### 3. Example of the MAC extended ACL

This example shows how to deny the host with the MAC address 00d0.f800.0c0c to provide service with the protocol type 100 on gigabitethernet port 1/1. The configuration procedure is as below:

```
Hostname(config)# access-list 702 deny host 00d0.f800.0c0c any aarp
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group 702 in
```

#### 4. Example of the expert extended ACL

The following example shows how to create and display an expert extended ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044.

```
Hostname(config)# access-list 2702 deny tcp host 192.168.12.3 mac
00d0.f800.0044 0000.0000.0000 any any
Hostname(config)# access-list 2702 permit any any any any
Hostname(config)# show access-lists
expert access-list extended 2702
10 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any
10 permit any any any any
```

| Related Commands | Command                  | Description        |
|------------------|--------------------------|--------------------|
|                  | <b>show access-lists</b> | Show all the ACLs. |

**Platform** N/A

**Description**

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** If the same ACE is added to an ACL repeatedly, the following error message is displayed:  
failed, for the entry is existed or the sequence number has been allocated!

**Common Errors** -

**Platform Description** -

## 1.2 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**access-list** *acl-id* **list-remark** *comment*

**no access-list** *acl-id* **list-remark**

| Parameter Description | Parameter      | Description                                                                                                                                                                         |
|-----------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>acl-id</i>  | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199. 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
|                       | <i>comment</i> | Comment that describes the access list.                                                                                                                                             |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.

**Configuration** The following example writes a comment of "this acl is to filter the host 192.168.4.12" for

**Examples**

ACL100.

```

Hostname(config)# ip access-list extended 100
Hostname(config)# access-list 100 list-remark this acl is to filter the
host 192.168.4.12

```

**Related Commands**

| Command                   | Description                                                            |
|---------------------------|------------------------------------------------------------------------|
| <b>show access- lists</b> | Displays all access lists, including the remarks for the access lists. |

**Verification**

Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications**

-

**Common Errors**

-

**Platform**

-

**Description**

## 1.3 access-list remark

Use this command to write a helpful comment (remark) for an entry in a numbered access list.

Use the **no** form of this command to remove the remark.

**access-list** *acl-id* [ *sn* ] **remark** *comment*

**no access-list** *acl-id* [ *sn* ] **remark** *comment*

**Parameter****Description**

| Parameter      | Description                                                                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl-id</i>  | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199, 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| <i>comment</i> | Comment that describes the access list entry.                                                                                                                                       |
| <i>sn</i>      | Indicates the sequence number of an ACE for which a comment is required.                                                                                                            |

**Defaults**

N/A

**Command Mode**

Global configuration mode

**Usage Guide**

You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.

**Configuration** The following example writes a comment for an entry in ACL102.

**Examples**

```
Hostname(config)# access-list 102 remark deny-host-10.1.1.1
```

| Related Commands | Command                  | Description                                                                   |
|------------------|--------------------------|-------------------------------------------------------------------------------|
|                  | <b>show access-lists</b> | Displays all access lists, including the remarks for the access list entries. |

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** N/A

## 1.4 clear counters access-list

Use this command to clear counters of packets matching ACLs.

**clear counters access-list** [ *id* | *name* ]

| Parameter Description | Parameter   | Description                                                                                                                                                                                                          |
|-----------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>id</i>   | ACL number. The following value ranges are supported:<br>IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899. |
|                       | <i>name</i> | ACL name. The value is a case-sensitive string of 1 to 99 characters.                                                                                                                                                |

### Defaults

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to clear the counters of packets matching the specified or all ACLs.

**Configuration** The following example clears the packet matching counter of ACL No. 2700:

**Examples**

```

Hostname #show access-lists 2700
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (88 matches)
 20 deny tcp any any eq login any any (33455 matches)
 30 permit tcp any any host 192.168.6.9 any (10 matches)

Hostname# clear counters access-list 2700
Hostname#show access-lists 2700

```

```
expert access-list extended 2700
 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
 20 deny tcp any any eq login any any
 30 permit tcp any any host 192.168.6.9 any
```

**Related  
Commands**

| Command            | Description                  |
|--------------------|------------------------------|
| expert access-list | Defines an expert ACL.       |
| deny               | Defines a deny ACL entry.    |
| permit             | Defines a permits ACL entry. |

**Platform** N/A  
**Description**

## 1.5 clear access-list counters

Use this command to clear counters of packets matching the deny entries in ACLs.

**clear access-list counters** [*id* | *name*]

**Parameter  
Description**

| Parameter   | Description                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>id</i>   | ACL number. The following value ranges are supported:<br>IP standard ACLs: 1 to 99 or 1300 to 1999; IP extended ACLs: 100 to 199 or 2000 to 2699; MAC extended ACLs: 700 to 799; expert extended ACLs: 2700 to 2899. |
| <i>name</i> | ACL name. The value is a case-sensitive string of 1 to 99 characters.                                                                                                                                                |

**Defaults**

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** This command is used to clear the counters of packets matching the deny entries in ACLs.

**Configuration** The following example clears the packet matching counter of ACL No. 1:

**Examples**

Before configuration:

```
Hostname#show access-lists
ip access-list standard 1
 10 deny host 50.1.1.2 (10 matches)
 20 permit host 60.1.1.2 (15 matches)
(10 packets filtered)
```



After configuration:

```

Hostname# end
Hostname# clear access-list counters
Hostname# show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)

```

#### Related Commands

| Command            | Description                  |
|--------------------|------------------------------|
| expert access-list | Defines an expert ACL.       |
| deny               | Defines a deny ACL entry.    |
| permit             | Defines a permits ACL entry. |

**Platform** N/A  
**Description**

## 1.6 deny

One or multiple **deny** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

### 1. Standard IP ACL

```
[ sn ] deny { source source-wildcard | host source | any } [ time-range time-range-name ] [ log ]
```

### 2. Extended IP ACL

```
[ sn ] deny protocol { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [ range lower upper ] [ time-range time-range-name ]
```

Extended IP ACLs of some important protocols:

- Internet Control Message Prot (ICMP)

```
[ sn ] deny icmp { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [ [ icmp-type [ icmp-code ] ] [ icmp-message ] ] [ time-range time-range-name ]
```

- Transmission Control Protocol (TCP)

```
[ sn ] deny tcp { source source-wildcard | host source | any } [ operator port [ port ] ] { destination destination-wildcard | host destination | any } [ operator port [ port ] ] [ range lower upper ] [ time-range time-range-name ]
```

- User Datagram Protocol (UDP)

```
[ sn ] deny udp { source source-wildcard | host source | any } [ operator port [ port ] ] { destination destination-wildcard | host destination | any } [ operator port [ port ] ] [ range lower upper ]
```

[ **time-range** *time-range-name* ]

### 3. Extended MAC ACL

[ *sn* ] **deny** { **any** | **host** *source-mac-address* / *source-mac-address* *source-mac-wildcard* } { **any** | **host** *destination-mac-address* } [ *ethernet-type* ] [ **cos** [ *cos* ] [ **inner** *cos* ] ] [ **time-range** *time-range-name* ]

### 4. Extended expert ACL

[ *sn* ] **deny** [ *protocol* | [ *ethernet-type* ] [ **cos** [ *cos* ] [ **inner** *cos* ] ] ] [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

- When you select the *ethernet-type* field or *cos* field:

[ *sn* ] **deny** { [ *ethernet-type* ] [ **cos** [ *cos* ] [ **inner** *cos* ] ] } [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ **time-range** *time-range-name* ]

- When you select the *protocol* field:

[ *sn* ] **deny** *protocol* [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

- Extended expert ACLs of some important protocols

#### Internet Control Message Protocol (ICMP)

[ *sn* ] **deny** **icmp** [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ [ *icmp-type* [ *icmp-code* ] ] ] [ [ *icmp-message* ] ] [ **time-range** *time-range-name* ]

#### Transmission Control Protocol (TCP)

[ *sn* ] **deny** **tcp** [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *Source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } [ *operator* *port* [ *port* ] ] { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ *operator* *port* [ *port* ] ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

#### User Datagram Protocol (UDP)

[ *sn* ] **deny** **udp** [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] { *source* *source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* } [ *operator* *port* [ *port* ] ] { *destination* *destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [ *operator* *port* [ *port* ] ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

#### Address Resolution Protocol (ARP)

[ *sn* ] **deny** **arp** [ [ **VID** [ *vid* ] [ **inner** *vid* ] ] ] [ **host** *source-mac-address* | **any** | *source-mac-address* *source-mac-wildcard* ] [ **host** *destination-mac-address* | **any** ] { *sender-ip* *sender-ip-wildcard* | **host** *sender-ip* | **any** } { *sender-mac* *sender-mac-wildcard* | **host** *sender-mac* | **any** } { *target-ip*

*target-ip-wildcard* | **host** *target-ip* | **any** } [ **time-range** *time-range-name* ]

#### 5. Extended IPv6 ACL

[ *sn* ] **deny** *protocol* { *source-ipv6-prefix* / *prefix-length* | **any** | **host** *source-ipv6-address* }  
 { *destination-ipv6-prefix* / *prefix-length* | **any** | **host** *destination-ipv6-address* } [ **flow-label** *flow-label* ]  
 [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

Extended ipv6 ACLs of some important protocols:

#### Internet Control Message Protocol (ICMP)

[ *sn* ] **deny** **icmp** { *source-ipv6-prefix* / *prefix-length* | **any** | **host** *source-ipv6-address* }  
 { *destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any** } [ [ *icmp-type*  
 [ *icmp-code* ] ] [ *icmp-message* ] ] [ **flow-label** *flow-label* ] [ **time-range** *time-range-name* ]

#### Transmission Control Protocol (TCP)

[ *sn* ] **deny** **tcp** { *source-ipv6-prefix* / *prefix-length* | **host** *source-ipv6-address* | **any** } [ *operator port*  
 [ *port* ] ] { *destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any** } [ *operator port*  
 [ *port* ] ] [ **flow-label** *flow-label* ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

#### User Datagram Protocol (UDP)

[ *sn* ] **deny** **udp** { *source-ipv6-prefix* / *prefix-length* | **host** *source-ipv6-address* | **any** } [ *operator port*  
 [ *port* ] ] { *destination-ipv6-prefix* / *prefix-length* | **host** *destination-ipv6-address* | **any** } [ *operator port*  
 [ *port* ] ] [ **flow-label** *flow-label* ] [ **range** *lower upper* ] [ **time-range** *time-range-name* ]

#### Parameter Description

| Parameter                       | Description                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <i>sn</i>                       | ACL entry sequence number                                                                                           |
| <i>source-ipv6-prefix</i>       | Source IPv6 network address or network type                                                                         |
| <i>destination-ipv6-prefix</i>  | Destination IPv6 network address or network type                                                                    |
| <i>prefix-length</i>            | Prefix mask length                                                                                                  |
| <i>source-ipv6-address</i>      | Source IPv6 address                                                                                                 |
| <i>destination-ipv6-address</i> | Destination IPv6 address                                                                                            |
| <b>cos</b> <i>cos</i>           | Class of service (0-7)                                                                                              |
| <b>cos inner</b> <i>cos</i>     | CoS of the packet tag                                                                                               |
| <b>VID</b> <i>vid</i>           | Match the specified VID.                                                                                            |
| <b>VID inner</b> <i>vid</i>     | Match the inner specified VID.                                                                                      |
| <b>range</b>                    | Layer4 port number range of the packet.                                                                             |
| <i>lower</i>                    | Lower limit of the layer4 port number.                                                                              |
| <i>upper</i>                    | Upper limit of the layer4 port number.                                                                              |
| <i>time-range-name</i>          | Time range name of packet filtering                                                                                 |
| <i>icmp-type</i>                | ICMP message type (0 to 255)                                                                                        |
| <i>icmp-code</i>                | ICMP message type code (0 to 255)                                                                                   |
| <i>icmp-message</i>             | ICMP message type name                                                                                              |
| <i>operator</i>                 | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)                                               |
| <b>flow-label</b>               | Flow label                                                                                                          |
| <i>flow-label</i>               | Flow label value, within the range of 0 to 1048575.                                                                 |
| <i>protocol</i>                 | For the IPv6, the field can be <i>ipv6</i>   <i>icmp</i>   <i>tcp</i>   <i>udp</i> and number in the range 0 to 255 |

|                        |                                                                  |
|------------------------|------------------------------------------------------------------|
| <b>time-range</b>      | Time range of the packet filtering                               |
| <i>time-range-name</i> | Time range name of the packet filtering                          |
| <b>log</b>             | Outputs the matching syslog when the packet matches the ACL rule |

**Defaults** No entry

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the filtering entry of ACLs in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```

Hostname(config)# expert access-list extended 2702
Hostname(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any
any
Hostname(config-exp-nacl)# permit any any any any
Hostname(config-exp-nacl)# show access-lists
expert access-list extended 2702
10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Hostname(config-exp-nacl)#

```

This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 0/1. The configuration procedure is as below:

```

Hostname(config)# ip access-list extended ip-ext-acl
Hostname(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group ip-ext-acl in
Hostname(config-if-GigabitEthernet 0/1)#

```

This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 0/1. The configuration procedure is as below:

```

Hostname(config)# mac access-list extended mac1
Hostname(config-mac-nacl)# deny host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)# exit

```

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group mac1 in

```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 0/1. The configuration procedure is as below:

```

Hostname(config)# ip access-list standard 34
Hostname(config-ext-nacl)# deny host 192.168.4.12
Hostname(config-ext-nacl)# show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Hostname(config-ext-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 34 in

```

This example shows how to use the extended IPv6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 0/1. The configuration procedure is as below:

```

Hostname(config)# ipv6 access-list extended v6-acl
Hostname(config-ipv6-nacl)# 11 deny ipv6 host 192.168.4.12 any
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
Hostname(config-ipv6-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in

```

#### Related Commands

| Command                    | Description                                     |
|----------------------------|-------------------------------------------------|
| <b>show access-lists</b>   | Displays all ACLs.                              |
| <b>ipv6 traffic-filter</b> | Applies the extended IPv6 ACL on the interface. |
| <b>ip access-group</b>     | Applies the IP ACL on the interface.            |
| <b>mac access-group</b>    | Applies the extended MAC ACL on the interface.  |
| <b>ip access-list</b>      | Defines an IP ACL.                              |
| <b>mac access-list</b>     | Defines an extended MAC ACL.                    |
| <b>expert access-list</b>  | Defines an extended expert ACL.                 |
| <b>ipv6 access-list</b>    | Defines an extended IPv6 ACL.                   |
| <b>permit</b>              | Permits the access.                             |

**Platform** N/A  
**Description**

## 1.7 expert access-group

Use this command to apply the specified expert access list on the specified interface to control the input and output data streams. Use the **no** form of the command to remove the application.

**expert access-group** { *acl-id* | *acl-name* } { **in** | **out** }

**no expert access-group** { *acl-id* | *acl-name* } { **in** | **out** }

| Parameter Description | Parameter       | Description                              |
|-----------------------|-----------------|------------------------------------------|
|                       | <i>acl-id</i>   | Expert access list number: 2700 to 2899  |
|                       | <i>acl-name</i> | Name of the expert access list           |
|                       | <b>in</b>       | Specifies filtering on inbound packets.  |
|                       | <b>out</b>      | Specifies filtering on outbound packets. |

**Defaults** No expert access list is applied.

**Command mode** Interface configuration mode.

**Usage Guide** To make an expert ACL take effect, run this command to apply the ACL in L3 Ethernet interface configuration mode.

**Configuration Examples** The following example applies the expert extended ACL named `accept_00d0f8xxxxxx_only` to the inbound direction of the L3 Ethernet interface GigabitEthernet 0/1.

```

Hostname(config)# interface GigaEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#          expert    access-group
accept_mac_only in

```

| Related Commands | Command                  | Description                     |
|------------------|--------------------------|---------------------------------|
|                  | <b>show access-group</b> | Displays the ACL configuration. |

**Platform Description** N/A

## 1.8 expert access-list extended

Use this command to create an expert extended access list. Use the **no** form of the command to remove the ACL.

**expert access-list extended** { *acl-id* | *acl-name* }

**no expert access-list extended** { *acl-id* | *acl-name* }

| Parameter   | Parameter       | Description                                      |
|-------------|-----------------|--------------------------------------------------|
| Description | <i>acl-id</i>   | Extended expert access list number: 2700 to 2899 |
|             | <i>acl-name</i> | Name of the expert extended access list          |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** Use the **show access-lists** command to display the ACL configurations.

**Configuration** Create an expert extended ACL named exp-acl:

**Examples**

```

Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
Hostname(config-exp-nacl)#

```

Create an expert extended ACL numbered 2704:

```

Hostname(config)# expert access-list extended 2704
Hostname(config-exp-nacl)# show access-lists
expert access-list extended 2704
Hostname(config-exp-nacl)#

```

| Related Commands | Command                  | Description                       |
|------------------|--------------------------|-----------------------------------|
|                  | <b>show access-lists</b> | Displays the expert extended ACLs |

**Verification**

**Notifications** -

**Common Errors** -

**Platform** -

**Description**

## 1.9 expert access-list resequence

Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.

**expert access-list resequence** { *acl-id* | *acl-name* } *start-sn inc-sn*

**no expert access-list resequence** { *acl-id* | *acl-name* }

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description |           |             |

|                 |                                                          |
|-----------------|----------------------------------------------------------|
| <i>acl-id</i>   | Expert access list number: 2700 to 2899.                 |
| <i>acl-name</i> | Name of the expert access list                           |
| <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
| <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**

*start-sn*: 10  
*inc-sn*: 10

**Command mode** Global configuration mode

**Usage Guide** To insert a new rule into an expert extended ACL, run this command to rearrange the sequence numbers of ACL rules.

**Configuration** The following example resequences entries of expert access list “exp-acl”:

**Examples**

Before the configuration:

```

Hostname# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any

```

After the configuration:

```

Hostname# config
Hostname(config)# expert access-list resequence exp-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any

```

**Related Commands**

| Command                  | Description                |
|--------------------------|----------------------------|
| <b>show access-lists</b> | Displays all access lists. |

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common Errors** -

**Platform** -

**Description** -



## 1.10 ip access-group

Use this command to apply a specific access list globally or to an interface or VXLAN. Use the **no** form of this command to remove the access list from the interface.

**ip access-group** { *acl-id* | *acl-name* } { **in** | **out** }

**no ip access-group** { *acl-id* | *acl-name* } { **in** | **out** }

### Parameter Description

| Parameter       | Description                                                                 |
|-----------------|-----------------------------------------------------------------------------|
| <i>acl-id</i>   | IP access list or extended IP access list number:<br>1 to 199, 1300 to 2699 |
| <i>acl-name</i> | Name of the IP ACL                                                          |
| <b>in</b>       | Filters the incoming packets of the interface.                              |
| <b>out</b>      | Filters the outgoing packets of the interface.                              |

### Defaults

N/A

### Command mode

Interface configuration mode.

### Usage Guide

To make an IP standard ACL or IP extended ACL take effect, run this command to apply the ACL in interface configuration mode.

### Configuration

#### Examples

The following example applies the ACL 120 on interface gigabitEthernet 0/1 to filter the incoming packets:

```

Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 120 in

```

### Related Commands

| Command                  | Description        |
|--------------------------|--------------------|
| <b>access-list</b>       | Defines an ACL.    |
| <b>show access-lists</b> | Displays all ACLs. |

### Verification

Run the **show ip access-group** command to check information about the IP standard ACL and IP extended ACL that have been applied.

Run the **show ip access-group** { **interface** *interface-name* | **wlan** *wlan-id* } command to check information about the IP standard ACL and IP extended ACL that have been applied to a specified interface or in WAN mode.

### Notifications

When a counter-only ACL is applied to a port, if an ACL (IP standard ACL, IP extended ACL, MAC extended ACL, or expert ACL) has been applied to the same direction of the port, the following notification will be displayed:

```

Another counter-only acl has attached at GigabitEthernet 0/1, Operation fail.

```

When a counter-only ACL is applied to a port, if the counter function of the ACL has been

enabled globally, the following notification will be displayed:

```
ACL 1 has been used as a traffic matching statistics ACL.
```

**Common Errors** -

**Platform** -

**Description** -

## 1.11 ip access-list

Use this command to create a standard IP access list or extended IP access list. Use the **no** form of the command to remove the access list.

```
ip access-list { extended | standard } { acl-id | acl-name }
```

```
no ip access-list { extended | standard } { acl-id | acl-name }
```

**Parameter Description**

| Parameter       | Description                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------|
| <i>acl-id</i>   | Access list number:<br>Standard: 1 to 99, 1300 to 1999;<br>Extended: 100 to 199, 2000 to 2699. |
| <i>acl-name</i> | Name of the access list                                                                        |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list. Refer to **deny** or **permit** in the two modes. Use the **show access-lists** command to display the ACL configurations.

**Configuration Examples** The following example creates a standard access list named std-acl.

```
Hostname(config)# ip access-list standard std-acl
Hostname(config-std-nacl)# show access-lists
ip access-list standard std-acl
Hostname(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
Hostname(config)# ip access-list extended 123
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 123
```

**Related Commands**

| Command                  | Description        |
|--------------------------|--------------------|
| <b>show access-lists</b> | Displays all ACLs. |

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** When you create a named IP standard or IP extended ACL, if the specified name has been used by another type of ACL, the following notification will be displayed:

```
ACL type error, current ACL has been set to type mac extended.
```

When you create a named IP standard or IP extended ACL, if the number of named ACLs (all types of named ACLs) created in the device has reached 500, the following notification will be displayed:

```
Failed to create user-defined acl for the max-limit has been reached
```

When you create a named IP standard or IP extended ACL, if the length of the name entered is longer than 99 characters, the following notification will be displayed:

```
Name is too long
```

When you create a named IP standard or IP extended ACL, if the entered name begins with a number or the name is in or out, the following notification will be displayed:

```
Invalid name
```

**Common Errors** -

**Platform** -

**Description**

## 1.12 ip access-list resequence

Use this command to resequence a standard or extended IP access list. Use the **no** form of this command to restore the default order of access entries.

**ip access-list resequence** { *acl-id* | *acl-name* } *start-sn inc-sn*

**no ip access-list resequence** { *acl-id* | *acl-name* }

| Parameter Description | Parameter       | Description                                                                                                                     |
|-----------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>acl-id</i>   | IP access list number:<br>Standard IP access list: 1 to 99, 1300 to 1999;<br>Extended IP access list: 100 to 199, 2000 to 2699. |
|                       | <i>acl-name</i> | Name of the standard or extended IP access list                                                                                 |
|                       | <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647                                                                                   |
|                       | <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647                                                                        |

**Defaults** *start-sn*: 10  
*inc-sn*: 10

**Command mode** Global configuration mode

**Usage Guide** To insert a new rule into an IP standard ACL or IP extended ACL, run this command to rearrange the sequence numbers of ACL rules.

**Configuration** The following example resequences entries of ACL1:

**Examples** Before the configuration:

```

Hostname# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any

```

After the configuration:

```

Hostname# config
Hostname(config)# ip access-list resequence 1 21 43
Hostname(config)# exit
Hostname# show access-lists
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any

```

**Related  
Commands**

| Command                  | Description                |
|--------------------------|----------------------------|
| <b>show access-lists</b> | Displays all access lists. |

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common  
Errors** -

**Platform  
Description** -

## 1.13 ipv6 access-list

Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the **no** form of this command to remove the access list.

```

ipv6 access-list acl-name
no ipv6 access-list acl-name

```

**Parameter  
Description**

| Parameter       | Description                   |
|-----------------|-------------------------------|
| <i>acl-name</i> | Name of the IPv6 access list. |

| <b>Defaults</b>               | N/A                                                                                                                                                                                                      |         |             |                          |                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------|--------------------------|----------------------------|
| <b>Command mode</b>           | Global configuration mode                                                                                                                                                                                |         |             |                          |                            |
| <b>Usage Guide</b>            | To filter IPv6 packets in the network, run this command to create an IPv6 ACL.                                                                                                                           |         |             |                          |                            |
| <b>Configuration Examples</b> | The following example creates an IPv6 access list named v6-acl:<br><pre> Hostname(config)# ipv6 access-list v6-acl Hostname(config-ipv6-nacl)# show access-lists ipv6 access-list extended v6-acl </pre> |         |             |                          |                            |
| <b>Related Commands</b>       | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show access-lists</b></td> <td>Displays all access lists.</td> </tr> </tbody> </table>          | Command | Description | <b>show access-lists</b> | Displays all access lists. |
| Command                       | Description                                                                                                                                                                                              |         |             |                          |                            |
| <b>show access-lists</b>      | Displays all access lists.                                                                                                                                                                               |         |             |                          |                            |
| <b>Verification</b>           | Run the <b>show access-lists</b> command on the device to display the comments configured for ACLs.                                                                                                      |         |             |                          |                            |
| <b>Notifications</b>          | -                                                                                                                                                                                                        |         |             |                          |                            |
| <b>Common Errors</b>          | -                                                                                                                                                                                                        |         |             |                          |                            |
| <b>Platform Description</b>   | -                                                                                                                                                                                                        |         |             |                          |                            |

## 1.14 ipv6 access-list resequence

Use this command to resequence an IPv6 access list. Use the **no** form of this command to restore the default order of access entries.

**ipv6 access-list resequence** *acl-name start-sn inc-sn*

**no ipv6 access-list resequence** *acl-name*

| Parameter Description | Parameter       | Description                                              |
|-----------------------|-----------------|----------------------------------------------------------|
|                       | <i>acl-name</i> | Name of the IPv6 access list                             |
|                       | <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
|                       | <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

|                     |                                            |
|---------------------|--------------------------------------------|
| <b>Defaults</b>     | <i>start-sn</i> : 10<br><i>inc-sn</i> : 10 |
| <b>Command mode</b> | Global configuration mode                  |

**Usage Guide** To insert a new rule into an IPv6 ACL, run this command to rearrange the sequence numbers of ACL rules.

**Configuration Examples** The following example configures an IPv6 ACL named v6-acl, sets the start value of rule sequence numbers to 21 and step to 43.

Before the configuration:

```

Hostname# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any

```

After the configuration:

```

Hostname# config
Hostname(config)# ipv6 access-list resequence v6-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any

```

**Related Commands**

| Command                  | Description                |
|--------------------------|----------------------------|
| <b>show access-lists</b> | Displays all access lists. |

**Platform** N/A

**Description**

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common** -

**Errors**

**Platform** -

**Description**

## 1.15 ipv6 traffic-filter

Use this command to apply an IPv6 access list on the specified interface/VXLAN. Use the **no** form of the command to remove the IPv6 access list from the interface/VXLAN.

**ipv6 traffic-filter** *acl-name* { **in** | **out** }

**no ipv6 traffic-filter** *acl-name* { **in** | **out** }

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>acl-name</i></td> <td>Name of IPv6 access list</td> </tr> <tr> <td><b>in</b></td> <td>Specifies filtering on inbound packets</td> </tr> <tr> <td><b>out</b></td> <td>Specifies filtering on outbound packets</td> </tr> </tbody> </table> | Parameter | Description | <i>acl-name</i>          | Name of IPv6 access list                      | <b>in</b> | Specifies filtering on inbound packets | <b>out</b> | Specifies filtering on outbound packets |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|--------------------------|-----------------------------------------------|-----------|----------------------------------------|------------|-----------------------------------------|
| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                          |           |             |                          |                                               |           |                                        |            |                                         |
| <i>acl-name</i>               | Name of IPv6 access list                                                                                                                                                                                                                                                                                                                             |           |             |                          |                                               |           |                                        |            |                                         |
| <b>in</b>                     | Specifies filtering on inbound packets                                                                                                                                                                                                                                                                                                               |           |             |                          |                                               |           |                                        |            |                                         |
| <b>out</b>                    | Specifies filtering on outbound packets                                                                                                                                                                                                                                                                                                              |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                                                                                                                                                                  |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Command mode</b>           | Interface configuration mode.                                                                                                                                                                                                                                                                                                                        |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Usage Guide</b>            | To make an IPv6 ACL take effect, run this command to apply the ACL in L3 Ethernet interface configuration mode,                                                                                                                                                                                                                                      |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Configuration Examples</b> | <p>The following example applies the IPv6 access list named <b>v6-acl</b> to interface GigabitEthernet 0/1:</p> <pre> Hostname(config)# interface GigaEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in </pre>                                                                                                     |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Related Commands</b>       | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show access-group</b></td> <td>Displays ACL configurations on the interface.</td> </tr> </tbody> </table>                                                                                                                                   | Command   | Description | <b>show access-group</b> | Displays ACL configurations on the interface. |           |                                        |            |                                         |
| Command                       | Description                                                                                                                                                                                                                                                                                                                                          |           |             |                          |                                               |           |                                        |            |                                         |
| <b>show access-group</b>      | Displays ACL configurations on the interface.                                                                                                                                                                                                                                                                                                        |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Verification</b>           | <p>Run the <b>show ipv6 traffic-filter</b> command to check the configuration of all IPv6 ACLs.</p> <p>Run the <b>show ipv6 traffic-filter { interface <i>interface-name</i> }</b> command to check the configuration of the IPv6 ACL that is applied to a specified interface.</p>                                                                  |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Notifications</b>          | -                                                                                                                                                                                                                                                                                                                                                    |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Common Errors</b>          | -                                                                                                                                                                                                                                                                                                                                                    |           |             |                          |                                               |           |                                        |            |                                         |
| <b>Platform Description</b>   | -                                                                                                                                                                                                                                                                                                                                                    |           |             |                          |                                               |           |                                        |            |                                         |

## 1.16 list-remark

Use this command to write a helpful comment (remark) for an access list. Use the **no** form of this command to remove the remark.

**list-remark** *comment*  
**no list-remark**

| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>comment</i></td> <td>Comment that describes the access list.</td> </tr> </tbody> </table> | Parameter | Description | <i>comment</i> | Comment that describes the access list. |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|----------------|-----------------------------------------|
| Parameter                    | Description                                                                                                                                                                                          |           |             |                |                                         |
| <i>comment</i>               | Comment that describes the access list.                                                                                                                                                              |           |             |                |                                         |

- Defaults** The access lists have no remarks by default.
- Command mode** ACL configuration mode
- Usage Guide** To view the function of an ACL conveniently in the future, run this command to add a remark to the ACL. You can also directly run the **access-list list-remark** command in global configuration mode to add a remark to an ACL.

**Configuration Examples** The following example writes a comment of “this acl is to filter the host 192.168.4.12” for ACL102.

```

Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# list-remark this acl is to filter the host
192.168.4.12
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
Hostname(config-ext-nacl)#

```

**Related Commands**

| Command                        | Description                                                             |
|--------------------------------|-------------------------------------------------------------------------|
| <b>show access-lists</b>       | Displays all access lists.                                              |
| <b>ip access-list</b>          | Defines an IPv4 access list.                                            |
| <b>access-list list remark</b> | Adds a helpful comment for an access list in global configuration mode. |

**Platform** N/A

**Description****Verification**

Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications**

-

**Common Errors**

-

**Platform****Description**

-

## 1.17 mac access-group

Use this command to apply the specified MAC access list on the specified interface. Use the **no** form of the command to remove the access list from the interface.

**mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }



**no mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }

**Parameter Description**

| Parameter       | Description                                           |
|-----------------|-------------------------------------------------------|
| <i>acl-id</i>   | MAC access list number. The range is from 700 to 799. |
| <i>acl-name</i> | Name of the MAC access list                           |
| <b>in</b>       | Specifies filtering on the inbound packets.           |
| <b>out</b>      | Specifies filtering on the outbound packets.          |

**Defaults** No MAC access list is applied by default.

**Command mode** interface configuration mode.

**Usage Guide** Use this command to apply the access list to filter the inbound or outbound packets based on the MAC address.

**Configuration Examples** The following example applies the MAC access-list **accept\_mac\_only** to interface GigabitEthernet 0/1:

```

Hostname(config)# interface gigaethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group accept_mac_only in

```

**Related Commands**

| Command                  | Description                                      |
|--------------------------|--------------------------------------------------|
| <b>show access-group</b> | Displays the ACL configuration on the interface. |

**Platform** N/A

**Description**

**Verification** Run the **show mac access-group** command to check application information about all MAC extended ACLs.

Run the **show mac access-group { interface *interface-name* | wlan *wlan-id* }** command to check information about the MAC extended ACL that has been applied to a specified interface.

**Notifications** -

**Common Errors** -

**Platform Description** -

## 1.18 mac access-list extended

Use this command to create an MAC extended access list. Use the **no** form of the command to remove the MAC access list.

**mac access-list extended** { *acl-id* | *acl-name* }

**no mac access-list extended** { *acl-id* | *acl-name* }

| Parameter Description | Parameter       | Description                                                    |
|-----------------------|-----------------|----------------------------------------------------------------|
|                       | <i>acl-id</i>   | Extended MAC access list number. The range is from 700 to 799. |
|                       | <i>acl-name</i> | Name of the MAC extended access list.                          |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** To filter L2 packets in the network, run this command to create a MAC extended ACL.

**Configuration Examples** The following example configures a MAC extended ACL named mac-acl.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended mac-acl
Hostname(config-mac-nacl)#

```

The following example configures a MAC extended ACL numbered 704.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# mac access-list extended 704
Hostname(config-mac-nacl)#

```

| Related Commands | Command                  | Description                |
|------------------|--------------------------|----------------------------|
|                  | <b>show access-lists</b> | Displays all access lists. |

**Platform** N/A

**Description**

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common Errors** -

**Platform**

-

## 1.19 mac access-list resequence

Use this command to resequence an MAC extended access list. Use the **no** form of this command to restore the default order of access entries.

**mac access-list resequence** { *acl-id* | *acl-name* } *start-sn* *inc-sn*

**no mac access-list resequence** { *acl-id* | *acl-name* }

**Parameter Description**

| Parameter       | Description                                              |
|-----------------|----------------------------------------------------------|
| <i>acl-id</i>   | Extended MAC access list number: 700 to 799.             |
| <i>acl-name</i> | Name of the MAC extended access list                     |
| <i>start-sn</i> | Start sequence number. Range: 1 to 2147483647            |
| <i>inc-sn</i>   | Increment of the sequence number. Range: 1 to 2147483647 |

**Defaults**

*start-sn*: 10

*inc-sn*: 10

**Command mode**

Global configuration mode

**Usage Guide**

To insert a new rule into a MAC extended ACL, run this command to rearrange the sequence numbers of ACL rules.

**Configuration Examples**

The following example configures a MAC extended ACL named mac-acl, sets the start value of rule sequence numbers to 21 and step to 43.

Before the configuration:

```

Hostname# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any

```

After the configuration:

```

Hostname# config
Hostname(config)# mac access-list resequence exp-acl 21 43
Hostname(config)# exit
Hostname# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any

```

| Related Commands | Command                  | Description                 |
|------------------|--------------------------|-----------------------------|
|                  | <b>show access-lists</b> | Displays all access lists.. |

**Platform** N/A

**Description**

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common** -

**Errors** -

**Platform** -

**Description** -

## 1.20 permit

One or multiple **permit** conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.

### 1. Standard IP ACL

```
[ sn ] permit { source source-wildcard | host source | any } [ time-range time-range-name ] [ log ]
```

### 2. Extended IP ACL

```
[ sn ] permit protocol { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [ range lower upper ] [ time-range time-range-name ]
```

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [ [ icmp-type [ icmp-code ] ] [ icmp-message ] ] [ time-range time-range-name ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp { source source-wildcard | host source | any } [ operator port [ port ] ] { destination destination-wildcard | host destination | any } [ operator port [ port ] ] [ range lower upper ] [ time-range time-range-name ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp { source source-wildcard | host source | any } [ operator port [ port ] ] { destination destination-wildcard | host destination | any } [ operator port [ port ] ] [ range lower upper ] [ time-range time-range-name ]
```

### 3. Extended MAC ACL

```
[ sn ] permit { any | host source-mac-address | source-mac-address source-mac-wildcard } { any | host destination-mac-address } [ ethernet-type ] [ cos [ cos ] [ inner cos ] ] [ time-range
```

*time-range-name* ]

#### 4. Extended expert ACL

```
[ sn ] permit [ protocol | [ ethernet-type ] [ cos [ cos ] [ inner cos ] ] ] [ VID [ vid ] [ inner vid ] ] { source
source-wildcard | host source | any } { host source-mac-address | any | source-mac-address
source-mac-wildcard } { destination destination-wildcard | host destination | any } { host
destination-mac-address | any } [ range lower upper ] [ time-range time-range-name ]
```

When you select the Ethernet-type field or cos field:

```
[ sn ] permit { ethernet-type / cos [ cos ] [ inner cos ] } [ VID [ vid ] [ inner vid ] ] { source
source-wildcard | host source | any } { host source-mac-address | any | source-mac-address
source-mac-wildcard } { destination destination-wildcard | host destination | any } { host
destination-mac-address | any } [ time-range time-range-name ]
```

When you select the protocol field:

```
[ sn ] permit protocol [ VID [ vid ] [ inner vid ] ] { source source-wildcard | host source | any } { host
source-mac-address | any | source-mac-address source-mac-wildcard } { destination
destination-wildcard | host destination | any } { host destination-mac-address | any } [ range lower
upper ] [ time-range time-range-name ]
```

Extended expert ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | host source | any } { host
source-mac-address | any | source-mac-address source-mac-wildcard } { destination
destination-wildcard | host destination | any } { host destination-mac-address | any } [ [ icmp-type
[ icmp-code ] ] | [ icmp-message ] ] [ time-range time-range-name ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | host source | any } { host
source-mac-address | any | source-mac-address source-mac-wildcard } [ operator port [ port ] ]
{ destination destination-wildcard | host destination | any } { host destination-mac-address | any }
[ operator port [ port ] ] [ range lower upper ] [ time-range time-range-name ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp [ VID [ vid ] [ inner vid ] ] { source source-wildcard | host source | any } { host
source-mac-address | any | source-mac-address source-mac-wildcard } [ operator port [ port ] ]
{ destination destination-wildcard | host destination | any } { host destination-mac-address | any }
[ operator port [ port ] ] [ range lower upper ] [ time-range time-range-name ]
```

Address Resolution Protocol (ARP)

```
[ sn ] permit arp [ VID [ vid ] [ inner vid ] ] { host source-mac-address | any | source-mac-address
source-mac-wildcard } { host destination-mac-address | any } { sender-ip sender-ip-wildcard | host
sender-ip | any } { sender-mac sender-mac-wildcard | host sender-mac | any } { target-ip
target-ip-wildcard | host target-ip | any } [ time-range time-range-name ]
```

#### 5. Extended IPv6 ACL

```
[ sn ] permit protocol { source-ipv6-prefix / prefix-length | any | host source-ipv6-address }
{ destination-ipv6-prefix / prefix-length | any | host destination-ipv6-address } [ flow-label flow-label ]
[ range lower upper ] [ time-range time-range-name ]
```

Extended IPv6 ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[ sn ] permit icmp { source-ipv6-prefix / prefix-length | any source-ipv6-address | host }
{ destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [ [ icmp-type
[ icmp-code ] ] [ icmp-message ] ] [ flow-label flow-label ] [ time-range time-range-name ]
```

Transmission Control Protocol (TCP)

```
[ sn ] permit tcp { source-ipv6-prefix / prefix-length | host source-ipv6-address | any } [ operator port
[ port ] ] { destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [ operator port
[ port ] ] [ flow-label flow-label ] [ range lower upper ] [ time-range time-range-name ]
```

User Datagram Protocol (UDP)

```
[ sn ] permit udp { source-ipv6-prefix / prefix-length | host source-ipv6-address | any } [ operator port
[ port ] ] { destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [ operator port
[ port ] ] [ flow-label flow-label ] [ range lower upper ] [ time-range time-range-name ]
```

#### Parameter Description

| Parameter                       | Description                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------|
| <i>sn</i>                       | ACL entry sequence number                                                               |
| <i>source-ipv6-prefix</i>       | Source IPv6 network address or network type                                             |
| <i>destination-ipv6-prefix</i>  | Destination IPv6 network address or network type                                        |
| <i>prefix-length</i>            | Prefix mask length                                                                      |
| <i>source-ipv6-address</i>      | Source IPv6 address                                                                     |
| <i>destination-ipv6-address</i> | Destination IPv6 address                                                                |
| <b>cos</b> <i>cos</i>           | Class of service (0-7)                                                                  |
| <b>cos inner</b> <i>cos</i>     | CoS of the packet tag                                                                   |
| <b>VID</b> <i>vid</i>           | Matches the specified VID                                                               |
| <b>VID inner</b> <i>vid</i>     | Matches the inner specified VID                                                         |
| <b>range</b>                    | Layer4 port number range of the packet                                                  |
| <i>lower</i>                    | Lower limit of the layer4 port number                                                   |
| <i>upper</i>                    | Upper limit of the layer4 port number                                                   |
| <i>time-range-name</i>          | Time range name of packet filtering                                                     |
| <i>icmp-type</i>                | ICMP message type (0 to 255)                                                            |
| <i>icmp-code</i>                | ICMP message type code (0 to 255)                                                       |
| <i>icmp-message</i>             | ICMP message type name                                                                  |
| <i>operator</i>                 | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)                   |
| <b>flow-label</b>               | Flow label                                                                              |
| <i>flow-label</i>               | Flow label value, within the range of 0 to 1048575.                                     |
| <i>protocol</i>                 | For the IPv6, the field can be ipv6   icmp   tcp   udp and number in the range 0 to 255 |
| <b>time-range</b>               | Time range of the packet filtering                                                      |
| <i>time-range-name</i>          | Time range name of the packet filtering                                                 |
| <b>log</b>                      | Outputs the matching syslog when the packet matches the ACL rule                        |

#### Defaults

N/A

**Command** ACL configuration mode.  
**mode**

**Usage Guide** Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

**Configuration Examples** The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272.

```
Hostname(config)# expert access-list extended exp-acl
Hostname(config-exp-nacl)# permit tcp host 192.168.4.12 host 0013.0049.8272
any any
Hostname(config-exp-nacl)# deny any any any any
Hostname(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
 10 permit tcp host 192.168.4.12 host 0013.0049.8272 any any
 20 deny any any any any
Hostname(config-exp-nacl)#
```

This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 0/1. The configuration procedure is as below:

```
Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# show access-lists
ip access-list extended 102
 10 permit tcp host 192.168.4.12 eq 100 any
Hostname(config-ext-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group 102 in
Hostname(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 0/1. The configuration procedure is as below:

```
Hostname(config)# mac access-list extended 702
Hostname(config-mac-nacl)# permit host 0013.0049.8272 any aarp
Hostname(config-mac-nacl)# show access-lists
mac access-list extended 702
 10 permit host 0013.0049.8272 any aarp 702
Hostname(config-mac-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 0/1. The configuration procedure is as below:

```
Hostname(config)# ip access-list standard std-acl
```

```

Hostname(config-std-nacl)# permit host 192.168.4.12
Hostname(config-std-nacl)# show access-lists
ip access-list standard std-acl
  10 permit host 192.168.4.12
Hostname(config-std-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip access-group std-acl in

```

This example shows how to use the extended IPv6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 0/1. The configuration procedure is as below:

```

Hostname(config)# ipv6 access-list extended v6-acl
Hostname(config-ipv6-nacl)# 11 permit ipv6 host ::192.168.4.12 any
Hostname(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any
Hostname(config-ipv6-nacl)# exit
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in

```

#### Related Commands

| Command                    | Description                                             |
|----------------------------|---------------------------------------------------------|
| <b>show access-lists</b>   | Displays all access lists.                              |
| <b>ipv6 traffic-filter</b> | Applies the extended IPv6 access list to the interface. |
| <b>ip access-group</b>     | Applies the IP access list to the interface.            |
| <b>mac access-group</b>    | Applies the extended MAC access list to the interface.  |
| <b>ip access-list</b>      | Defines an IP access list.                              |
| <b>mac access-list</b>     | Defines an extended MAC access list.                    |
| <b>expert access-list</b>  | Define an extended expert access list.                  |
| <b>ipv6 access-list</b>    | Defines an extended IPv6 access list.                   |
| <b>deny</b>                | Defines the <b>deny</b> access entry.                   |

**Platform** N/A  
**Description**

## 1.21 remark

Use this command to write a helpful comment (remark) for an entry in the access list. Use the **no** form of this command to remove the remark.

**[ sn ] remark comment**

**no [ sn ] remark comment**



| Parameter Description | Parameter      | Description                                                                                                   |
|-----------------------|----------------|---------------------------------------------------------------------------------------------------------------|
|                       | <i>comment</i> | Comment that describes the access entry.                                                                      |
|                       | <i>sn</i>      | Sequence number of an ACL rule, to which a remark needs to be added. The value range is from 1 to 2147483647. |

**Defaults** The access entries have no remarks.

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to write a helpful comment for an access entry.  
Up to 100 characters are allowed in the remark.  
Two identical access entry remarks in one access list is not allowed.  
Removing an access entry may delete the remark for it as well.

**Configuration Examples** The following example writes remarks for the entry in extended IP access list 102.

```

Hostname(config)# ip access-list extended 102
Hostname(config-ext-nacl)# remark first_remark
Hostname(config-ext-nacl)# 10 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Hostname(config-ext-nacl)# 10 remark second_remark
Hostname(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Hostname(config-ext-nacl)# end

```

| Related Commands | Command                  | Description                |
|------------------|--------------------------|----------------------------|
|                  | <b>show access-lists</b> | Displays all access lists. |
|                  | <b>ip access-list</b>    | Defines an IP access list. |

**Platform** N/A

**Description**

**Verification** Run the **show access-lists** command on the device to display the comments configured for ACLs.

**Notifications** -

**Common Errors** -

**Platform Description** -

## 1.22 security access-group

Use this command to configure an interface secure channel. Use the **no** form of this command to remove the channel.

**security access-group** { *acl-id* | *acl-name* }

**no security access-group**

### Parameter Description

| Parameter       | Description                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl-id</i>   | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199, 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| <i>acl-name</i> | Name of the access list.                                                                                                                                                            |

### Defaults

N/A

### Command mode

Interface configuration mode

### Usage Guide

If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.

### Configuration Examples

The following example configures a secure channel on interface gigabitethernet 0/1:

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security access-group 1
```

### Related Commands

| Command              | Description                                |
|----------------------|--------------------------------------------|
| <b>show secu-acl</b> | Displays the secure channel configuration. |

### Verification

N/A

### Notifications

-

### Common Errors

-

### Platform Description

-

## 1.23 security global access-group

Use this command to configure the global secure channel.

**security global access-group** { *acl-id* | *acl-name* }  
**no security global access-group**

**Parameter  
Description**

| Parameter       | Description                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl-id</i>   | Access list number.<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199. 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| <i>acl-name</i> | Name of the access list.                                                                                                                                                            |

**Defaults**

N/A

**Command mode**

Global configuration mode

**Usage Guide**

If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.

**Configuration**

The following example configures a global secure channel.

**Examples**

```
Hostname(config)# security global access-group 1
```

**Related Commands**

| Command              | Description                                |
|----------------------|--------------------------------------------|
| <b>show secu-acl</b> | Displays the secure channel configuration. |

**Verification**

N/A

**Notifications**

-

**Common Errors**

-

**Platform Description**

-

## 1.24 security uplink enable

Use this command to configure an exceptional interface of the global secure channel.

**security uplink enable**  
**no security uplink enable**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|     |     |
|-----|-----|
| N/A | N/A |
|-----|-----|

**Defaults** The global secure channel takes effect on all interfaces by default.

**Command mode** Interface configuration mode.

**Usage Guide** The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can use this command to configure the interface as exceptional.

**Configuration Examples** The following example configures interface gigabitethernet 0/1 as an exceptional interface of the secure channel.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# security uplink enable

```

| Related Commands | Command              | Description                                |
|------------------|----------------------|--------------------------------------------|
|                  | <b>show secu-acl</b> | Displays the secure channel configuration. |

**Verification** N/A

**Notifications** -

**Common Errors** -

**Platform** -

**Description** -

## 1.25 show access-group

Use this command to display the access list applied to the interface.

**show access-group** [ **interface** *interface-name* | **wlan** *wlan-id* ]

| Parameter Description | Parameter                  | Description                          |
|-----------------------|----------------------------|--------------------------------------|
|                       | <i>interface-name</i>      | Interface name                       |
|                       | <b>wlan</b> <i>wlan-id</i> | WLAN ID in the range from 1 to 4,094 |

**Defaults** -

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the access list configuration on the specified interface. If no interface is

specified, access list configuration on all interfaces is displayed.

**Configuration** The following example displays the interfaces where the ACL is applied.

**Examples**

```

Hostname# show access-group
ip access-list standard ipstd3 in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out

```

The following example displays whether ACL is applied on the interface GigabitEthernet 0/1 and which direction data streams flow to.

```

Hostname# show access-group interface GigabitEthernet 0/1
ip access-list extended 101
Applied On interface GigabitEthernet 0/1 in.

```

**Related  
Commands**

| Command                    | Description                                      |
|----------------------------|--------------------------------------------------|
| <b>ip access-group</b>     | Applies the IP access list to the interface.     |
| <b>mac access-group</b>    | Applies the MAC access list to the interface.    |
| <b>expert access-group</b> | Applies the expert access list to the interface. |

**Platform** N/A

**Description**

## 1.26 show access-lists

Use this command to display all access lists or the specified access list.

**show access-lists** [ *acl-id* | *acl-name* ] [ **summary** ]

**Parameter  
Description**

| Parameter       | Description                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl-id</i>   | Access list number<br>Standard IP ACL: 1 to 99, 1300 to 1999.<br>Extended IP ACL: 100 to 199, 2000 to 2699.<br>Extended MAC ACL: 700 to 799.<br>Extended Expert ACL: 2700 to 2899. |
| <i>acl-name</i> | Name of the access list                                                                                                                                                            |
| <b>summary</b>  | Access list summary                                                                                                                                                                |

**Defaults** N/A

**Command mode** Global configuration mode

**Usage Guide** Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.

**Configuration** The following example displays configuration of the ACL named "n\_acl".

**Examples**

```

Hostname# show access-lists n_acl
ip access-list standard n_acl
Hostname# show access-lists 102
ip access-list extended 102

```

The following example displays configuration of all ACLs.

```

Hostname# show access-lists
ip access-list standard n_acl
ip access-list extended 101
permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-aclipv6 access-list extended v6-acl
petmit ipv6 100::2 any (100 matches)
deny any any (9 matches)

```

**Related  
Commands**

| Command                   | Description                             |
|---------------------------|-----------------------------------------|
| <b>ip access-list</b>     | Defines an IP access list.              |
| <b>mac access-list</b>    | Defines an MAC extended access list.    |
| <b>expert access-list</b> | Defines an expert extended access list. |
| <b>ipv6 access-list</b>   | Defines an extended IPv6 access list.   |

**Platform** N/A

**Description**

## 1.27 show expert access-group

Use this command to display the expert access list applied to the interface.

**show expert access-group** [ **interface** *interface-name* | **wlan** *wlan-id* ]

**Parameter  
Description**

| Parameter                  | Description                          |
|----------------------------|--------------------------------------|
| <i>Interface-name</i>      | Interface name                       |
| <b>wlan</b> <i>wlan-id</i> | WLAN ID in the range from 1 to 4,094 |

**Defaults**

-

**Command** Privileged EXEC mode  
**mode**

**Usage Guide** Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.

**Configuration Examples** The following example displays information about the expert extended ACL applied to the L3 Ethernet interface GigabitEthernet 0/1.

```

Hostname# show expert access-group interface gigabitethernet 0/1
expert access-group ee in
Applied On interface GigabitEthernet 0/1.

```

**Related Commands**

| Command                   | Description                             |
|---------------------------|-----------------------------------------|
| <b>expert access-list</b> | Defines an expert extended access list. |

**Platform** N/A  
**Description**

## 1.28 show ip access-group

Use this command to display the standard and extended IP access lists on the interface.

**show ip access-group [ interface *interface-name* | wlan *wlan-id* ]**

**Parameter Description**

| Parameter                  | Description                          |
|----------------------------|--------------------------------------|
| <i>Interface-name</i>      | Interface name                       |
| <b>wlan</b> <i>wlan-id</i> | WLAN ID in the range from 1 to 4,094 |

**Defaults** N/A

**Command** Privileged EXEC mode  
**mode**

**Usage Guide** Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.

**Configuration Examples** The following example displays whether the standard or extended IP access list is applied on the interface GigabitEthernet 0/1 and which direction data streams flow to.

```

Hostname# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.

```

| Related Commands | Command               | Description                |
|------------------|-----------------------|----------------------------|
|                  | <b>ip access-list</b> | Defines an IP access list. |

**Platform** N/A  
**Description**

## 1.29 show ipv6 traffic-filter

Use this command to display the IPv6 access list on the interface.

**show ipv6 traffic-filter** [ **interface** *interface-name* ]

| Parameter Description | Parameter             | Description    |
|-----------------------|-----------------------|----------------|
|                       | <i>Interface-name</i> | Interface name |

**Defaults** This command is used to display the IPv6 ACL applied to a port. If no port is specified, the IPv6 ACLs applied to all ports are displayed.

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.

**Configuration Examples** The following example displays whether IPv6 ACL is applied on the interface GigabitEthernet 0/1 and which direction data streams flow to.

```

Hostname# show ipv6 traffic-filter interface gigabitethernet 0/1
ipv6 access-group v6 in
Applied On interface GigabitEthernet 0/1.

```

| Related Commands | Command                 | Description                  |
|------------------|-------------------------|------------------------------|
|                  | <b>ipv6 access-list</b> | Defines an IPv6 access list. |

**Platform** N/A  
**Description**

## 1.30 show mac access-group

Use this command to display the MAC access list on the interface.

**show mac access-group** [ **interface** *interface-name* | **wlan** *wlan-id* ]



| Parameter<br>Description | Parameter             | Description                          |
|--------------------------|-----------------------|--------------------------------------|
|                          | <i>Interface-name</i> | Interface name                       |
|                          | <i>Wlan wlan-id ]</i> | WLAN ID in the range from 1 to 4,094 |

**Defaults** N/A

**Command mode** Privileged EXEC mode

**Usage Guide** Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.

**Configuration Examples** The following example displays the MAC access list is applied on the interface and which direction data streams flow to.

```

Hostname# show mac access-group interface gigabitethernet 0/1
mac access-group mm in
Applied On interface GigabitEthernet 0/1.

```

| Related<br>Commands | Command                | Description                |
|---------------------|------------------------|----------------------------|
|                     | <b>mac access-list</b> | Defines a MAC access list. |

**Platform Description** N/A

# 1 ARP-Check Commands

## 1.1 arp-check

Use this command to enable the ARP check function on the Layer 2 interface.

Use the **no** form of this command to restore the default setting.

**arp-check**

**no arp-check**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command mode** Interface configuration mode/WLAN security configuration mode

**Usage Guide** The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.

**Configuration Examples** This following example enables the APR check function on interface GigabitEthernet 0/1 and WLAN1.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp-check
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# arp-check
Hostname(config-wlansec)# end

```

| Related Commands | Command                              | Description                     |
|------------------|--------------------------------------|---------------------------------|
|                  | <b>show interface arp-check list</b> | Displays the ARP check entries. |

**Platform Description** N/A

## 1.2 show interfaces arp-check list

Use this command to display the ARP check entries on the Layer 2 interface.

**show { interfaces [ interface-type interface-number ] | wlan [ wlan-id ] } arp-check list**

| Parameter Description | Parameter               | Description            |
|-----------------------|-------------------------|------------------------|
|                       | <i>interface-type</i>   | Wired interface type   |
|                       | <i>interface-number</i> | Wired interface number |
|                       | <i>wlan-id</i>          | WLAN ID                |

**Command mode** All modes except the user EXEC mode

**Usage** Use this command to display the ARP check entries.

**Guide**

**Configuration** The following example displays the ARP check entries.

```

Examples
Hostname# show interfaces arp-check list
INTERFACE                SENDER MAC      SENDER IP      POLICY SOURCE
-----
GigabitEthernet 0/1      00D0.F800.0003  192.168.1.3    address-bind
GigabitEthernet 0/1      00D0.F800.0001  192.168.1.1    port-security
Hostname(config)#show wlan arp-check list
INTERFACE                SENDER MAC      SENDER IP      POLICY SOURCE
-----
WLAN 1                   00D0.F800.0008  192.168.1.8    DHCP snooping
    
```

| Field         | Description         |
|---------------|---------------------|
| INTERFACE     | Interface name      |
| SENDER MAC    | Source MAC address  |
| SENDER IP     | Source IP address   |
| POLICY SOURCE | Source of the entry |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

# 1 Anti-ARP Spoofing Commands

## 1.1 anti-arp-spoofing ip

Use this command to enable anti-ARP spoofing.

Use the **no** form of this command to disable this function.

**anti-arp-spoofing ip** *ipv4-address*

**no anti-arp-spoofing ip** *ipv4-address*

| Parameter Description | Parameter           | Description          |
|-----------------------|---------------------|----------------------|
|                       | <i>ipv4-address</i> | Gateway IPv4 address |

**Defaults** The anti-ARP spoofing function is disabled by default.

**Command Mode** WLAN security configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables anti-ARP spoofing.

```

Hostname# configure terminal
Hostname(config)# wlansec 1
Hostname(config-wlansec)# anti-arp-spoofing ip 192.168.1.1

```

| Related Commands | Command                       | Description                                   |
|------------------|-------------------------------|-----------------------------------------------|
|                  | <b>show anti-arp-spoofing</b> | Displays the anti-ARP spoofing configuration. |

**Platform** N/A

**Description**

## 1.2 show anti-arp-spoofing

Use this command to display the anti-ARP spoofing configuration on all interfaces.

**show anti-arp-spoofing**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** This command is used to display the anti-ARP spoofing configuration on all interfaces.

**Configuration** The following example displays the anti-ARP-spoofing configuration on all interfaces.

**Examples**

```

Hostname# show anti-arp-spoofing
NO      PORT      IP          STATUS
-----
1       Gi0/1      192.168.1.1 active
    
```

Field Description

| Field  | Description              |
|--------|--------------------------|
| NO     | Order number             |
| PORT   | Port number              |
| IP     | Gateway IP               |
| STATUS | Anti-ARP spoofing status |

| Related Commands | Command                     | Description |
|------------------|-----------------------------|-------------|
|                  | <b>anti-arp-spoofing ip</b> |             |

**Platform Description** N/A

# 1 Global IP-MAC Binding Address Commands

## 1.1 address-bind

Use this command to configure global IP-MAC address binding. Use the **no** form of this command to restore the default setting.

**address-bind** { *ipv4-address* | *ipv6-address* } *mac-address*

**no address-bind** { *ipv4-address* | *ipv6-address* } *mac-address*

| Parameter   | Parameter           | Description              |
|-------------|---------------------|--------------------------|
| Description | <i>ipv4-address</i> | IPv4 address to be bound |
|             | <i>ipv6-address</i> | IPv6 address to be bound |
|             | <i>mac-address</i>  | MAC address to be bound  |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example configures global IP-MAC address binding.

```

Hostname# configure terminal
Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001

```

| Related Commands | Command                  | Description                                        |
|------------------|--------------------------|----------------------------------------------------|
|                  | <b>show address-bind</b> | Displays the IP address-MAC address binding table. |

**Platform** N/A

**Description**

## 1.2 address-bind install

Use this command to enable a binding policy globally. Use the **no** form of this command to restore the default setting.

**address-bind install**

**no address-bind install**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** If you bind an IP address to a MAC address, run this command to make the installation policy take effect.

**Configuration** The following example enables a binding policy.

**Examples**

```
Hostname# configure terminal
Hostname(config)# address-bind 192.168.5.1 00d0.f800.0001
Hostname(config)# address-bind install
```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

**Platform** N/A

**Description**

### 1.3 address-bind ipv6-mode

This command is used to set the IPv6 address binding mode. Use the **no** form of this command to restore the default setting.

This command is also used to set the compatible mode.

**address-bind ipv6-mode { compatible | loose | strict }**

**no address-bind ipv6-mode**

| Parameter   | Parameter         | Description     |
|-------------|-------------------|-----------------|
| Description | <b>compatible</b> | Compatible mode |
|             | <b>loose</b>      | Loose mode      |
|             | <b>strict</b>     | Strict mode     |

**Defaults** The default is strict mode.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the IPv6 address binding mode.

**Examples**

```
Hostname# configure terminal
Hostname(config)# address-bind ipv6-mode compatible
```

| Related  | Command                         | Description                                           |
|----------|---------------------------------|-------------------------------------------------------|
| Commands | <b>show address-bind uplink</b> | Displays the exceptional port of the address binding. |

Platform N/A

Description

## 1.4 address-bind uplink

This command is used to configure the exception port. Use the **no** form of this command to restore the default setting.

**address-bind uplink** *interface-id*

**no address-bind uplink** *interface-id*

| Parameter   | Parameter           | Description                               |
|-------------|---------------------|-------------------------------------------|
| Description | <i>interface-id</i> | Switching port or layer 2 aggregate port. |

Defaults All ports are non-exception ports by default.

Command Global configuration mode.

Mode

Usage Guide If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address.

If the port is an exceptional port and is installed (see `address-bind install`), this binding policy does not take effect.

Configuration The following example configures the exception port.

```
Examples
Hostname# configure terminal
Hostname(config)# address-bind uplink gigabitethernet 0/1
```

| Related  | Command                         | Description                                       |
|----------|---------------------------------|---------------------------------------------------|
| Commands | <b>show address-bind uplink</b> | Displays the exceptional port of address binding. |

Platform N/A

Description

## 1.5 show address-bind

Use this command to display global IP address-MAC address binding.

**show address-bind**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|



|                     |                       |     |
|---------------------|-----------------------|-----|
| <b>Description</b>  | N/A                   | N/A |
| <b>Defaults</b>     | N/A                   |     |
| <b>Command Mode</b> | Privileged EXEC mode. |     |
| <b>Usage Guide</b>  | N/A                   |     |

**Configuration** The following example displays global IPv4 address-MAC address binding.

**Examples**

```

Hostname# show address-bind
Total Bind Addresses in System : 1
IP Address      Binding MAC Addr
-----
192.168.5.1    00d0.f800.0001
    
```

| Field                          | Description                            |
|--------------------------------|----------------------------------------|
| Total Bind Addresses in System | IPv4 address-MAC address binding count |
| IP Address                     | Bound IP address                       |
| Binding MAC Addr               | Bound MAC address                      |

| Related Commands | Command             | Description                             |
|------------------|---------------------|-----------------------------------------|
|                  | <b>address-bind</b> | Enables IP address-MAC address binding. |

**Platform** N/A  
**Description**

## 1.6 show address-bind uplink

Use this command to display the exception port.

**show address-bind uplink**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A  
**Command mode** N/A  
**Usage Guide** N/A

**Configuration** The following example displays the exception port.

**Examples**

```

Hostname# show address-bind uplink
    
```

| Field | Description                                                                                                                                       |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Port  | Short for exception ports. All ports are non-exception ports by default.                                                                          |
| State | Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it is not. |

| Related Commands | Command                    | Description              |
|------------------|----------------------------|--------------------------|
|                  | <b>address-bind uplink</b> | Sets the exception port. |

**Platform** N/A  
**Description**

# 1 IP Source Guard Commands

## 1.1 ip source binding

Use this command to add static user information to IP source address binding database.

Use the **no** form of this command to delete static user information from IP source address binding database.

**ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* { **interface** *interface-type* *interface-number* | **wlan** *wlan-id* | **ip-mac** | **ip-only** }


**no ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* { **interface** *interface-type* *interface-number* | **wlan** *wlan-id* | **ip-mac** | **ip-only** }

| Parameter Description | Parameter                                        | Description                                                                                                         |
|-----------------------|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
|                       | <i>mac-address</i>                               | Adds user MAC address statically.                                                                                   |
|                       | <i>vlan-id</i>                                   | Adds user VLAN ID statically. For products that support QinQ termination, it refers to the outer VLAN ID of a user. |
|                       | <i>ip-address</i>                                | Adds user IP address statically.                                                                                    |
|                       | <i>interface-type</i><br><i>interface-number</i> | Adds user interface ID statically.                                                                                  |
|                       | <b>wlan</b> <i>wlan-id</i>                       | Add user WLAN ID statically.                                                                                        |
|                       | <b>ip-mac</b>                                    | The global binding type is IP+MAC                                                                                   |
|                       | <b>ip-only</b>                                   | The global binding type is IP only.                                                                                 |

**Defaults** No static address is added by default.

**Command Mode** Global configuration mode

**Usage Guide** This command allows specific clients to go through IP source guard detection instead of DHCP. This command is supported on the wired L2 switching port, AP port, sub interface and WLAN. This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.

 A static IPv6 source binding is valid either on wired and WLAN interfaces or in global configuration mode.

 A new binding will overwrite the old one sharing the same configuration.

**Configuration Examples** The following example adds the interface Id and WLAN ID of static users.

```

Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface

```

```

gigabitethernet 0/1
Hostname(config)# ip source binding 0000.0000.0002 vlan 1 1.1.1.2 wlan 1
Hostname(config)# end

```

The following example adds static user information based on IP-MAC binding.

```

Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
Hostname(config)# end

```

The following example adds static user information based on IP binding.

```

Hostname# configure terminal
Hostname(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Hostname(config)# end

```

#### Related Commands

| Command                       | Description                                                         |
|-------------------------------|---------------------------------------------------------------------|
| <b>show ip source binding</b> | Displays the binding information of IP source address and database. |

**Platform** N/A  
**Description**

## 1.2 ip verify source

Use this command to enable IP Source Guard function on the interface.

Use the **no** form of this command to restore the default setting.

**ip verify source [ port-security ]**

**no ip verify source**

#### Parameter Description


| Parameter            | Description                                              |
|----------------------|----------------------------------------------------------|
| <b>port-security</b> | Configures IP Source Guard to do IP+MAC-based detection. |

**Defaults** This function is disabled by default.

**Command Mode** Interface configuration mode/WLAN security configuration mode

**Usage Guide** This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection.

This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

 IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by

## DHCP Snooping.

**Configuration**

The following example enables IP-based IP Source Guard function.

**Examples**

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
Hostname(config-if)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# ip verify source
Hostname(config-wlansec)# end

```

The following example enables IP+MAC-based IP Source Guard function.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source port-security
Hostname(config-if)# exit
Hostname(config)# wlansec 1
Hostname(config-wlansec)# ip verify source port-security
Hostname(config-wlansec)# end

```

**Related  
Commands**

| Command                      | Description                                       |
|------------------------------|---------------------------------------------------|
| <b>show ip verify source</b> | Displays user filtering entry of IP Source Guard. |

**Platform**

N/A

**Description**

## 1.3 ip verify source exclude-vlan

Use this command to exclude a VLAN from the IP source guard configuration on the port.

Use the **no** form of this command to restore the function.

**ip verify source exclude-vlan** *vlan-id*

**no ip verify source exclude-vlan** *vlan-id*

**Parameter  
Description**

| Parameter      | Description                                                     |
|----------------|-----------------------------------------------------------------|
| <i>vlan-id</i> | The ID of VLAN excluded from the IP source guard configuration. |

**Defaults**

This function is disabled by default.


**Command  
Mode**

Interface configuration mode/WLAN security configuration mode

**Usage Guide** This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered.

Once the IP source guard function is disabled, the excluded VLAN is cleared automatically.

This command is supported on the wired L2 switching port, AP port, sub interface and WLAN.

 Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.

**Configuration Examples** The following example configuration configures the IP source guard configuration for the port and excludes a VLAN.

```

Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip verify source
Hostname(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 2
Hostname(config-if)# end
Hostname(config)# wlansec 1
Hostname(config-wlansec)# ip verify source
Hostname(config-wlansec)# ip verify exclude-vlan 2
Hostname(config-wlansec)# end

```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.4 show ip source binding

Use this command to display the binding information of IP source addresses and database.

**show ip source binding** [ *ip-address* ] [ *mac-address* ] [ **dhcp-snooping** ] [ **static** ] [ **vlan** *vlan-id* ] [ **interface** *interface-id* ]

**Parameter Description**

| Parameter            | Description                                                   |
|----------------------|---------------------------------------------------------------|
| <i>ip-address</i>    | Displays user binding information of corresponding IP.        |
| <i>mac-address</i>   | Displays user binding information of corresponding MAC.       |
| <b>dhcp-snooping</b> | Displays binding information of dynamic user.                 |
| <b>static</b>        | Displays binding information of static user.                  |
| <i>vlan-id</i>       | Displays user binding information of corresponding VLAN.      |
| <i>interface-id</i>  | Displays user binding information of corresponding interface. |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode****Usage Guide** N/A**Configuration Examples** The following example displays the binding information of IP source guard addresses and database.

```

Hostname# show ip source binding static
Total number of bindings: 5
NO.    MACADDRESS          IPADDRESS    LEASE (SEC)  TYPE        VLAN  INTERFACE
-----
1      0001.0002.0001       1.2.3.2     Infinite     Static      1     Global
2      0001.0002.0002       1.2.3.3     Infinite     Static      1     GigabitEthernet
0/1
3      0001.0002.0003       1.2.3.4     Infinite     Static      1     Global
4      0001.0002.0004       1.2.3.5     Infinite     Static      1     Global
5      0001.0002.0005       1.2.3.6     Infinite     Static      1     WLAN 1

```

**Related Commands**

| Command                  | Description                   |
|--------------------------|-------------------------------|
| <b>ip source binding</b> | Sets the binding static user. |

**Platform** N/A**Description**

## 1.5 show ip verify source

Use this command to display user filtering entry of IP Source Guard.

**show ip verify source** [ **interface** *interface-type interface-number* ] [ **wlan** *wlan-id* ]

**Parameter Description**

| Parameter                                        | Description                                               |
|--------------------------------------------------|-----------------------------------------------------------|
| <i>interface-type</i><br><i>interface-number</i> | Displays user filtering entry of corresponding interface. |
| <i>wlan-id</i>                                   | Displays user filtering entry of corresponding WLAN.      |

**Defaults** N/A**Command Mode** Privileged EXEC mode**Usage Guide** If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: "IP source guard is not configured on the interface FastEthernet 0/10"  
Now, IP Source Guard supports the following filtering modes:

**inactive-restrict-off:** the IP Source Guard is disabled on bound interfaces.

**inactive-not-apply:** the IP Source Guard cannot adds bound entries into filtering entries for system errors.

**active:** the IP Source Guard is active.

**Configuration** The following example displays user filtering entry of IP Source Guard.

```

Examples
Hostname# show ip verify source
Total number of bindings: 7
NO.   INTERFACE          FILTERTYPE  FILTERSTATUS      IPADDRESS
MACADDRESS  VLAN  TYPE
-----
-----
1     Global              IP+MAC     Inactive-not-apply 192.168.0.127
0001.0002.0003 1 Static
2     GigabitEthernet 0/1 IP-ONLY     Active             1.2.3.4
0001.0002.0004 1 DHCP-Snooping
3     Global              IP-ONLY     Active             1.2.3.7
0001.0002.0007 1 Static
4     Global              IP+MAC     Active             1.2.3.6
0001.0002.0006 1 Static
    
```

| Related Commands | Command | Description             |
|------------------|---------|-------------------------|
|                  |         | <b>ip verify source</b> |

**Platform** N/A  
**Description**



# 1 CPP Commands

## 1.1 cpu-protect type pps

Use this command to set the bandwidth for receiving packets of a specified type for on the CPU port.

Use the **no** form of this command to restore the default setting.

```
cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client |  
dhcp-relay-server | dhcps | igmp | ipmc | ipv6-nans | lldp | ospf | ospfv3 | pim | pppoe | rip |  
ripng | vrrp } pps value
```

```
no cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client |  
dhcp-relay-server | dhcps | igmp | ipmc | ipv6-nans | lldp | ospf | ospfv3 | pim | pppoe | rip |  
ripng | vrrp } pps
```

**Parameter  
Description**

| Parameter         | Description                                                                              |
|-------------------|------------------------------------------------------------------------------------------|
| arp               | ARP packets.                                                                             |
| bpdu              | IEEE BPDU packets.                                                                       |
| capwap-disc       | CAPWAP Discover packets.                                                                 |
| d1x               | 802.1x EAPOL packets.                                                                    |
| dhcp-option82     | DHCP option82 packets.                                                                   |
| dhcp-relay-client | DHCP relay client packets.                                                               |
| dhcp-relay-server | DHCP relay server packets.                                                               |
| dhcps             | DHCP Snooping packets.                                                                   |
| igmp              | IGMP packets.                                                                            |
| ipmc              | IPv4 multicast packets.                                                                  |
| ipv6-nans         | IPv6 neighbor discovery packets.                                                         |
| lldp              | LLDP packets.                                                                            |
| ospf              | OSPF packets.                                                                            |
| ospfv3            | OSPF version 3 packets.                                                                  |
| pim               | PIM packets.                                                                             |
| pppoe             | PPPOE packets.                                                                           |
| rip               | IPv4 RIP packets.                                                                        |
| ripng             | IPv6 RIP packets.                                                                        |
| vrrp              | VRRP packets.                                                                            |
| <i>value</i>      | Number of received packets per second, in the range from 0 to 148810 in the unit of pps. |

**Defaults** The default value is 128.

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the CPU's bandwidth for receiving ARP packets to 200pps.

**Examples** `Hostname(config)# cpu-protect type arp pps 200`

| Command                                                   | Description                                                                    |
|-----------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>cpu-protect type packet-type pri</b><br><i>pri_num</i> | Sets the priority of the packets of a specified type received by the CPU port. |

**Platform** N/A  
**Description**

## 1.2 show cpu-protect summary

Use this command to display bandwidth of packets of each type received on the CPU port.  
show cpu-protect summary

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

The following example displays bandwidth of packets of each type received on the CPU port.

```

Hostname# show cpu-protect summary
Type                Pps
-----
arp                  100
dlx                  128
bpdu                 128
lldp                 128
dhcp-relay-server   128
dhcp-relay-client   128
dhcps                128
dhcp-option82       128
capwap-disc         128
ipv6-nans            128
rip                  128
pppoe                128
ripng                600
ospf                 600
ospfv3               600
    
```

**Configuration**  
**Examples**

|      |      |
|------|------|
| vrrp | 128  |
| igmp | 200  |
| pim  | 1000 |
| ipmc | 128  |

| Field | Description |
|-------|-------------|
| Type  | Packet type |
| Pps   | Bandwidth   |

Related Command

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

Platform Description N/A

### 1.3 show cpu-protect type

Use this command to display statistics about the packets of a specified type.

**show cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client | dhcp-relay-server | dhcps | igmp | ipmc | ipv6-nans | lldp | ospf | ospfv3 | pim | pppoe | rip | ripng | vrrp }**

Parameter Description

| Parameter         | Description                      |
|-------------------|----------------------------------|
| arp               | ARP packets.                     |
| bpdu              | IEEE BPDU packets.               |
| capwap-disc       | CAPWAP Discover packets.         |
| d1x               | 802.1x EAPOL packets.            |
| dhcp-option82     | DHCP Option82 packets.           |
| dhcp-relay-client | DHCP relay client packets.       |
| dhcp-relay-server | DHCP relay server packets.       |
| dhcps             | DHCP Snooping packets.           |
| igmp              | IGMP packets.                    |
| ipmc              | IPv4 multicast packets.          |
| ipv6-nans         | IPv6 neighbor discovery packets. |
| lldp              | LLDP packets.                    |
| ospf              | OSPF packets.                    |
| ospfv3            | OSPF version 3 packets.          |
| pim               | PIM packets.                     |
| pppoe             | PPPOE packets.                   |
| rip               | IPv4 RIP packets.                |
| ripng             | IPv6 RIP packets.                |
| vrrp              | VRRP packets.                    |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

The following example displays statistics about received BPDU packets.

**Configuration Examples**

```

Hostname# show cpu-protect type arp
Type                Pps          Total        Drop
-----
arp                 100          1611254     121265
    
```

| Field | Description                      |
|-------|----------------------------------|
| Type  | Packet type                      |
| Pps   | Bandwidth                        |
| Total | Total number of received packets |
| Drop  | Total number of lost packets     |

**Related Command**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

# 1 NFPP Commands

## 1.1 arp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

**no arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** }

**default arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** | **per-port** }

| Parameter Description | Parameter          | Description                                                            |
|-----------------------|--------------------|------------------------------------------------------------------------|
|                       | <b>per-src-ip</b>  | Sets the attack threshold for each source IP address.                  |
|                       | <b>per-src-mac</b> | Sets the attack threshold for each source MAC address.                 |
|                       | <b>per-port</b>    | Sets the attack threshold for each port.                               |
|                       | <i>pps</i>         | Sets the attack threshold, in the range from 1 to 9999 in unit of pps. |

**Defaults** By default, the attack threshold for each source IP address and source MAC address is 60pps; and the attack threshold for each port is 480pps.

**Command Mode** NFPP configuration mode

**Usage Guide** The attack threshold shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the global attack threshold.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Hostname(config-nfpp)# arp-guard attack-threshold per-port 50
```

| Related Commands | Command                            | Description                                             |
|------------------|------------------------------------|---------------------------------------------------------|
|                  | <b>nfpp arp-guard policy</b>       | Displays the rate-limit threshold and attack threshold. |
|                  | <b>show nfpp arp-guard summary</b> | Displays the configuration.                             |
|                  | <b>show nfpp arp-guard hosts</b>   | Displays the monitored host.                            |
|                  | <b>clear nfpp arp-guard hosts</b>  | Clears the isolate host.                                |

**Platform** N/A

## Description

## 1.2 arp-guard enable

Use this command to enable anti-ARP guard function globally. Use the **no** form of this command to disable anti-ARP guard. Use the **default** form of this command to restore the default setting.

**arp-guard enable**

**no arp-guard enable**

**default arp-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables anti-ARP guard function globally.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard enable

```

| Related Commands | Command                            | Description                               |
|------------------|------------------------------------|-------------------------------------------|
|                  | <b>nfpp arp-guard enable</b>       | Enables ARP anti-attack on the interface. |
|                  | <b>show nfpp arp-guard summary</b> | Displays the configuration.               |

**Platform** N/A

**Description**

## 1.3 arp-guard isolate-period

Use this command to set the arp-guard isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard isolate-period { seconds | permanent }**

**no arp-guard isolate-period**

**default arp-guard isolate-period**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|                  |                                                                                                 |
|------------------|-------------------------------------------------------------------------------------------------|
| <i>seconds</i>   | Sets the isolate time. The value is 0, or in the range from 30 to 86400 in the unit of seconds. |
| <b>permanent</b> | Permanent isolation.                                                                            |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the arp-guard isolate time globally to 180 seconds.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard isolate-period 180

```

**Related Commands**

| Command                              | Description                             |
|--------------------------------------|-----------------------------------------|
| <b>nfpp arp-guard isolate-period</b> | Sets the isolate time on the interface. |
| <b>show nfpp arp-guard summary</b>   | Displays the configuration.             |

**Platform** N/A

**Description**

## 1.4 arp-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard monitored-host-limit** *number*

**no arp-guard monitored-host-limit**

**default arp-guard monitored-host-limit**

**Parameter Description**

| Parameter     | Description                                                               |
|---------------|---------------------------------------------------------------------------|
| <i>number</i> | The maximum number of monitored hosts, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command Mode** NFPP configuration mode

**Usage Guide** If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts. to

remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that %NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to remind the administrator.

**Configuration** The following example sets the maximum number of monitored hosts to 200.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitored-host-limit 200

```

**Related Commands**

| Command                            | Description                 |
|------------------------------------|-----------------------------|
| <b>show nfpp arp-guard summary</b> | Displays the configuration. |

**Platform** N/A

**Description**

## 1.5 arp-guard monitor-period

Use this command to configure the arp guard monitor time. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard monitor-period** *seconds*

**no arp-guard monitor-period**

**default arp-guard monitor-period**

**Parameter Description**

| Parameter      | Description                                                                   |
|----------------|-------------------------------------------------------------------------------|
| <i>seconds</i> | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration** The following example sets the arp-guard monitor time to 180 seconds.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard monitor-period 180

```



| Related<br>Commands | Command                            | Description                       |
|---------------------|------------------------------------|-----------------------------------|
|                     | <b>show nfpp arp-guard summary</b> | Displays the configuration.       |
|                     | <b>show nfpp arp-guard hosts</b>   | Displays the monitored host list. |
|                     | <b>clear nfpp arp-guard hosts</b>  | Clears the isolate host.          |

Platform N/A

Description

## 1.6 arp-guard rate-limit

Use this command to set the arp-guard rate limit. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

**no arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** }

**default arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** }

| Parameter<br>Description | Parameter          | Description                                      |
|--------------------------|--------------------|--------------------------------------------------|
|                          | <b>per-src-ip</b>  | Sets the rate limit for each source IP address.  |
|                          | <b>per-src-mac</b> | Sets the rate limit for each source MAC address. |
|                          | <b>per-port</b>    | Sets the rate limit for each port.               |
|                          | <i>pps</i>         | Sets the rate limit, in the range of 1 to 9999.  |

**Defaults** The default rate limit for each source IP address and MAC address is 30pps; the default rate limit for each port is 240pps.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the arp guard rate limit.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# arp-guard rate-limit per-src-mac 3
Hostname(config-nfpp)# arp-guard rate-limit per-port 50

```

| Related<br>Commands | Command                            | Description                                   |
|---------------------|------------------------------------|-----------------------------------------------|
|                     | <b>nfpp arp-guard policy</b>       | Sets the rate limit and the attack threshold. |
|                     | <b>show nfpp arp-guard summary</b> | Displays the configuration.                   |

**Platform** N/A

**Description**

## 1.7 arp-guard scan-threshold

Use this command to set the global scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard scan-threshold** *pkt-cnt*

**no arp-guard scan-threshold**

**default arp-guard scan-threshold**

| Parameter Description | Parameter      | Description                                           |
|-----------------------|----------------|-------------------------------------------------------|
|                       | <i>pkt-cnt</i> | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** The default scan threshold is 100, in 10 seconds.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** The scanning may occur on the condition that:  
 more than 15 packets are received within 10 seconds;  
 the source MAC address for the link layer is constant while the source IP address is uncertain;  
 The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.

**Configuration** The following example sets the global scan threshold to 20pps.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard scan-threshold 20
  
```

| Related Commands | Command                              | Description                          |
|------------------|--------------------------------------|--------------------------------------|
|                  | <b>nfpp arp-guard scan-threshold</b> | Sets the scan threshold on the port. |
|                  | <b>show nfpp arp-guard summary</b>   | Displays the configuration.          |
|                  | <b>show nfpp arp-guard scan</b>      | Displays the ARP guard scan table.   |
|                  | <b>clear nfpp arp-guard scan</b>     | Clears the ARP guard scan table.     |

**Platform** N/A

**Description**

## 1.8 arp-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**arp-guard trusted-host** *ip mac*

**no arp-guard trusted-host** { **all** | *ip mac* }

**default arp-guard trusted-host**

| Parameter Description | Parameter  | Description                |
|-----------------------|------------|----------------------------|
|                       | <i>ip</i>  | Sets the IP address.       |
|                       | <i>mac</i> | Sets the MAC address.      |
|                       | <b>all</b> | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the ARP packets are sent from the trusted host to CPU without rate limit or alarm notification.  
Up to 500 hosts are supported.

**Configuration Examples** The following example sets the host whose IP address and MAC address are 1.1.1.1 and 0000.0000.1111 respectively as the trusted host.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# arp-guard trusted-host 1.1.1.1 0000.0000.1111
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.9 clear nfpp arp-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp arp-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-type interface-num* ] [ *ip-address* | *mac-address* ]

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|                                     |                                     |
|-------------------------------------|-------------------------------------|
| <i>vid</i>                          | Sets the VLAN ID.                   |
| <i>interface-type interface-num</i> | Sets the interface type and number. |
| <i>ip-address</i>                   | Sets the IP address.                |
| <i>mac-address</i>                  | Sets the MAC address.               |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide**

**Configuration Examples** The following example clears the monitored hosts of ARP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname# clear nfpp arp-guard hosts vlan 1 interface gigabitethernet 0/1
```

**Related Commands**

| Command                           | Description                                    |
|-----------------------------------|------------------------------------------------|
| <b>arp-guard attack-threshold</b> | Sets the global attack threshold.              |
| <b>nfpp arp-guard policy</b>      | Sets the limit threshold and attack threshold. |
| <b>show nfpp arp-guard hosts</b>  | Displays the monitored host.                   |

**Platform** N/A

**Description**

## 1.10 clear nfpp arp-guard scan

Use this command to clear ARP scanning table.

**clear nfpp arp-guard scan**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example clears ARP scanning table.

```
Hostname# clear nfpp arp-guard scan
```

| Related<br>Commands | Command                           | Description                       |
|---------------------|-----------------------------------|-----------------------------------|
|                     | <b>arp-guard attack-threshold</b> | Sets the global attack threshold. |
|                     | <b>nfpp arp-guard policy</b>      | Sets the attack threshold.        |
|                     | <b>show nfpp arp-guard scan</b>   | Displays the ARP scanning table.  |

**Platform** N/A

**Description**

## 1.11 clear nfpp dhcp-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp dhcp-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-type interface-num* ] [ *mac-address* ]

| Parameter<br>Description | Parameter                           | Description                         |
|--------------------------|-------------------------------------|-------------------------------------|
|                          | <i>vid</i>                          | Sets the VLAN ID.                   |
|                          | <i>interface-type interface-num</i> | Sets the interface type and number. |
|                          | <i>mac-address</i>                  | Sets the MAC address.               |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored hosts of DHCP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname# clear nfpp dhcp-guard hosts vlan 1 interface gigabitethernet 0/1
```

| Related<br>Commands | Command                            | Description                                    |
|---------------------|------------------------------------|------------------------------------------------|
|                     | <b>dhcp-guard attack-threshold</b> | Sets the global attack threshold.              |
|                     | <b>nfpp dhcp-guard policy</b>      | Sets the limit threshold and attack threshold. |
|                     | <b>show nfpp dhcp-guard hosts</b>  | Displays the monitored host.                   |

**Platform** N/A

**Description**

## 1.12 clear nfpp dhcpv6-guard hosts

Use this command to clear the monitored host isolation.

```
clear nfpp dhcpv6-guard hosts [ vlan vid ] [ interface interface-type interface-num ] [ mac-address ]
```

| Parameter Description | Parameter                           | Description                         |
|-----------------------|-------------------------------------|-------------------------------------|
|                       | <i>vid</i>                          | Sets the VLAN ID.                   |
|                       | <i>interface-type interface-num</i> | Sets the interface type and number. |
|                       | <i>mac-address</i>                  | Sets the MAC address.               |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** Use this command without the parameter to clear all monitored hosts

**Configuration** The following example clears the monitored hosts of DHCPv6 guard on VLAN 1 interface

**Examples** GigabitEthernet 0/1.

```
Hostname# clear nfpp dhcpv6-guard hosts vlan 1 interface gigabitethernet 0/1
```

| Related Commands | Command                              | Description                                    |
|------------------|--------------------------------------|------------------------------------------------|
|                  | <b>dhcpv6-guard attack-threshold</b> | Sets the global attack threshold.              |
|                  | <b>nfpp dhcpv6-guard policy</b>      | Sets the limit threshold and attack threshold. |
|                  | <b>show nfpp dhcpv6-guard hosts</b>  | Displays the monitored host.                   |

**Platform** N/A

**Description**

## 1.13 clear nfpp icmp-guard hosts

Use this command to clear the monitored host isolation.

```
clear nfpp icmp-guard hosts [ vlan vid ] [ interface interface-type interface-num ] [ ip-address ]
```

| Parameter Description | Parameter                           | Description                         |
|-----------------------|-------------------------------------|-------------------------------------|
|                       | <i>vid</i>                          | Sets the VLAN ID.                   |
|                       | <i>interface-type interface-num</i> | Sets the interface type and number. |
|                       | <i>ip-address</i>                   | Sets the IP address.                |

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored hosts of ICMP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname# clear nfpp icmp-guard hosts vlan 1 interface gigabitethernet 0/1
```

| Related Commands | Command                            | Description                                    |
|------------------|------------------------------------|------------------------------------------------|
|                  | <b>icmp-guard attack-threshold</b> | Sets the global attack threshold.              |
|                  | <b>nfpp icmp-guard policy</b>      | Sets the limit threshold and attack threshold. |
|                  | <b>show nfpp icmp-guard hosts</b>  | Displays the monitored host.                   |

**Platform** N/A  
**Description**

## 1.14 clear nfpp ip-guard hosts

Use this command to clear the monitored host isolation.

**clear nfpp ip-guard hosts** [ **vlan** *vid* ] [ **interface** *interface-type interface-num* ] [ *ip-address* ]

| Parameter Description | Parameter                           | Description                         |
|-----------------------|-------------------------------------|-------------------------------------|
|                       | <i>vid</i>                          | Sets the VLAN ID.                   |
|                       | <i>interface-type interface-num</i> | Sets the interface type and number. |
|                       | <i>ip-address</i>                   | Sets the IP address.                |

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** Use this command without the parameter to clear all monitored hosts.

**Configuration Examples** The following example clears the monitored hosts of IP guard on VLAN 1 interface GigabitEthernet 0/1.

```
Hostname# clear nfpp ip-guard hosts vlan 1 interface gigabitethernet 0/1
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|------------------|---------|-------------|

|                                  |                                                |
|----------------------------------|------------------------------------------------|
| <b>ip-guard attack-threshold</b> | Sets the global attack threshold.              |
| <b>nfpp ip-guard policy</b>      | Sets the limit threshold and attack threshold. |
| <b>show nfpp ip-guard hosts</b>  | Displays the monitored host.                   |

**Platform** N/A

**Description**

## 1.15 clear nfpp log

Use this command to clear the NFPP log buffer.

**clear nfpp log**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example clears the NFPP log buffer.

**Examples**

```
Hostname# clear nfpp log
32 log-buffer entries were cleared.
```

| Related Commands | Command              | Description                                            |
|------------------|----------------------|--------------------------------------------------------|
|                  | <b>show nfpp log</b> | Displays the NFPP log configuration or the log buffer. |

**Platform** N/A

**Description**

## 1.16 cpu-protect sub-interface percent

Use this command to configure the percent value of each type of packets that occupy queues.

**cpu-protect sub-interface** { *manage* | *protocol* | *route* } **percent** *percent-value*

Use the **no** form of this command to delete the percent value of each type of packets that occupy queues and restore default settings.

**no cpu-protect sub-interface** { *manage* | *protocol* | *route* } **percent**



Use the **default** form of this command to restore the default configuration.

**default cpu-protect sub-interface** { *manage* | *protocol* | *route* } **percent**

| Parameter<br>Description | Parameter             | Description                                                                                             |
|--------------------------|-----------------------|---------------------------------------------------------------------------------------------------------|
|                          | <b>manage</b>         | Specifies management packets.                                                                           |
|                          | <b>protocol</b>       | Specifies protocol packets.                                                                             |
|                          | <b>route</b>          | Specifies routing packets.                                                                              |
|                          | <i>percent-valeur</i> | Specifies the percentage of each type of packets that occupy queues.<br>The value ranges from 1 to 100. |

**Defaults** The percent value of management packets that occupy queues in the buffer is 30%.  
The percent value of routing packets that occupy queues in the buffer is 40%.  
The percent value of protocol packets that occupy queues in the buffer is 25%.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example sets the percent value of management packets in the buffer to 60.

**Examples**

```
Hostname(config)# cpu-protect sub-interface manage percent 60
```

**Verification** -

**Notifications** -

**Common** -

**Errors**

**Platform** -

**Description**

## 1.17 cpu-protect sub-interface pps

Use this command to configure the traffic bandwidth of each type of packets.

**cpu-protect sub-interface** { *manage* | *protocol* | *route* } **pps** *pps-valeur*

Use the **no** form of this command to delete the traffic bandwidth of each type of packets and restore default settings.

**no cpu-protect sub-interface** { *manage* | *protocol* | *route* } **pps**

Use the **default** form of this command to restore the default configuration.

**default cpu-protect sub-interface** { *manage* | *protocol* | *route* } **pps**

| Parameter Description | Parameter        | Description                                          |
|-----------------------|------------------|------------------------------------------------------|
|                       | <b>manage</b>    | Specifies management packets.                        |
|                       | <b>protocol</b>  | Specifies protocol packets.                          |
|                       | <b>route</b>     | Specifies routing packets.                           |
|                       | <i>pps-value</i> | Specifies the threshold in the range of 1 to 100000. |

**Defaults** The default settings of this command depend on the product version.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example configures the bandwidth of management packets as 2000 pps.

**Examples**

```
Hostname(config)# cpu-protect sub-interface manage pps 2000
```

**Verification** -

**Notifications** -

**Common** -

**Errors**

**Platform** -

**Description**

## 1.18 dhcp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard attack-threshold** { *per-src-mac* | *per-port* } *pps*

**no dhcp-guard attack-threshold** { *per-src-mac* | *per-port* }

**default dhcp-guard attack-threshold** { *per-src-mac* | *per-port* }

| Parameter Description | Parameter          | Description                                                               |
|-----------------------|--------------------|---------------------------------------------------------------------------|
|                       | <b>per-src-mac</b> | Sets the attack threshold for each source MAC address.                    |
|                       | <b>per-port</b>    | Sets the attack threshold for each port.                                  |
|                       | <i>pps</i>         | Sets the attack threshold in the range from 1 to 9999 in the unit of pps. |

**Defaults** By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the global attack threshold.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Hostname(config-nfpp)# dhcp-guard attack-threshold per-port 200

```

| Related Commands | Command                             | Description                                             |
|------------------|-------------------------------------|---------------------------------------------------------|
|                  | <b>nfpp dhcp-guard policy</b>       | Displays the rate-limit threshold and attack threshold. |
|                  | <b>show nfpp dhcp-guard summary</b> | Displays the configuration.                             |
|                  | <b>show nfpp dhcp-guard hosts</b>   | Displays the monitored host list.                       |
|                  | <b>clear nfpp dhcp-guard hosts</b>  | Clears the monitored host.                              |

**Platform Description** N/A

## 1.19 dhcp-guard enable

Use this command to enable the DHCP anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard enable**

**no dhcp-guard enable**

**default dhcp-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the DHCP anti-attack function.

```

Examples
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard enable

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.20 dhcp-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

```

dhcp-guard isolate-period { seconds | permanent }
no dhcp-guard isolate-period
default dhcp-guard isolate-period

```

| Parameter Description | Parameter      | Description          |
|-----------------------|----------------|----------------------|
|                       | <i>seconds</i> |                      |
| <b>permanent</b>      |                | Permanent isolation. |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

**Configuration** The following example sets the isolate time globally to 180 seconds.

```

Examples
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard isolate-period 180

```

| Related<br>Commands | Command                               | Description                             |
|---------------------|---------------------------------------|-----------------------------------------|
|                     | <b>nfpp dhcp-guard isolate-period</b> | Sets the isolate time on the interface. |
|                     | <b>show nfpp dhcp-guard summary</b>   | Displays the configuration.             |

Platform N/A

Description

## 1.21 dhcp-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard monitored-host-limit** *number*

**no dhcp-guard monitored-host-limit**

**default dhcp-guard monitored-host-limit**

| Parameter<br>Description | Parameter     | Description                                                               |
|--------------------------|---------------|---------------------------------------------------------------------------|
|                          | <i>number</i> | The maximum number of monitored hosts, in the range from 1 to 4294967295. |

Defaults The default is 1000.

Command NFPP configuration mode  
Mode

**Usage Guide** If the number of monitored hosts has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts. to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum number of monitored hosts has been exceeded, it prompts the message that %NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to remind the administrator.

**Configuration** The following example sets the maximum number of monitored hosts to 200.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitored-host-limit 200

```

| Related<br>Commands | Command                             | Description                 |
|---------------------|-------------------------------------|-----------------------------|
|                     | <b>show nfpp dhcp-guard summary</b> | Displays the configuration. |

Platform N/A

## Description

## 1.22 dhcp-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard monitor-period** *seconds*

**no dhcp-guard monitor-period**

**default dhcp-guard monitor-period**

| Parameter Description | Parameter      | Description                                                                   |
|-----------------------|----------------|-------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration** The following example sets the monitor time to 180 seconds.

**Examples**

```
Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard monitor-period 180
```

| Related Commands | Command                             | Description                       |
|------------------|-------------------------------------|-----------------------------------|
|                  | <b>show nfpp dhcp-guard summary</b> | Displays the configuration.       |
|                  | <b>show nfpp dhcp-guard hosts</b>   | Displays the monitored host list. |
|                  | <b>clear nfpp dhcp-guard hosts</b>  | Clears the isolate host.          |

**Platform** N/A

**Description**

## 1.23 dhcp-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command

to restore the default setting.

**dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps*

**no dhcp-guard rate-limit** { **per-src-mac** | **per-port** }

**default dhcp-guard rate-limit** { **per-src-mac** | **per-port** }

| Parameter Description | Parameter          | Description                                      |
|-----------------------|--------------------|--------------------------------------------------|
|                       | <b>per-src-mac</b> | Sets the rate limit for each source MAC address. |
|                       | <b>per-port</b>    | Sets the rate limit for each port.               |
|                       | <i>pps</i>         | Sets the rate limit, in the range of 1 to 9999.  |

**Defaults** The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
Hostname(config-nfpp)# dhcp-guard rate-limit per-port 100

```

| Related Commands | Command                             | Description                                   |
|------------------|-------------------------------------|-----------------------------------------------|
|                  | <b>nfpp dhcp-guard policy</b>       | Sets the rate limit and the attack threshold. |
|                  | <b>show nfpp dhcp-guard summary</b> | Displays the configuration.                   |

**Platform Description** N/A

## 1.24 dhcp-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**dhcp-guard trusted-host** *mac*

**no dhcp-guard trusted-host** { **all** | *mac* }

**default dhcp-guard trusted-host**

| Parameter Description | Parameter  | Description           |
|-----------------------|------------|-----------------------|
|                       | <i>mac</i> | Sets the MAC address. |

|            |                            |
|------------|----------------------------|
| <b>all</b> | Deletes all trusted hosts. |
|------------|----------------------------|

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the DHCP packets are sent from the trusted host to CPU without rate limit or alarm notification.  
Up to 500 trusted hosts are supported.

**Configuration Examples** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

```

Hostname (config) # nfpp
Hostname (config-nfpp) #dhcp-guard trusted-host 0000.0000.1111
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.25 dhcpv6-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

```

dhcpv6-guard attack-threshold { per-src-mac | per-port } pps
no dhcpv6-guard attack-threshold {per-src-mac | per-port}
default dhcpv6-guard attack-threshold { per-src-mac | per-port}
    
```

| Parameter Description | Parameter                                                      | Description                                            |
|-----------------------|----------------------------------------------------------------|--------------------------------------------------------|
|                       | <b>per-src-mac</b>                                             | Sets the attack threshold for each source MAC address. |
| <b>per-port</b>       | Sets the attack threshold for each port.                       |                                                        |
| <i>pps</i>            | Sets the attack threshold, in the range is from 1 to 9999 pps. |                                                        |

**Defaults** By default, the attack threshold for each source MAC address is 10pps; and the attack threshold for each port is 300pps

**Command Mode** NFPP configuration mode

**Usage Guide** N/A



**Configuration** The following example sets the global attack threshold.

```

Examples
Hostname (config) # nfpp
Hostname (config-nfpp) # dhcpv6-guard attack-threshold per-src-mac 15
Hostname (config-nfpp) # dhcpv6-guard attack-threshold per-port 200
    
```

| Related Commands | Command                               | Description                                             |
|------------------|---------------------------------------|---------------------------------------------------------|
|                  | <b>nfpp dhcpv6-guard policy</b>       | Displays the rate-limit threshold and attack threshold. |
|                  | <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.                             |
|                  | <b>show nfpp dhcpv6-guard hosts</b>   | Displays the monitored host list.                       |
|                  | <b>clear nfpp dhcpv6-guard hosts</b>  | Clears the monitored host.                              |

**Platform** N/A

**Description**

## 1.26 dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

- dhcpv6-guard enable**
- no dhcpv6-guard enable**
- default dhcpv6-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example enables the DHCPv6 anti-attack function globally.

```

Examples
Hostname (config) # nfpp
Hostname (config-nfpp) # dhcpv6-guard enable
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.27 dhcpv6-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard isolate-period** { *seconds* | **permanent** }

**no dhcpv6-guard isolate-period**

**default dhcpv6-guard isolate-period**

| Parameter Description | Parameter        | Description                                                                                       |
|-----------------------|------------------|---------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i>   | Sets the isolate time. The value is 0 or in the range is from 30 to 86400 in the unit of seconds. |
|                       | <b>permanent</b> | Permanent isolation.                                                                              |

**Defaults** The default is 0 second, which means no isolation.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

**Configuration** The following example sets the isolate time globally to 180 seconds.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard isolate-period 180

```

| Related Commands | Command                                 | Description                             |
|------------------|-----------------------------------------|-----------------------------------------|
|                  | <b>nfpp dhcpv6-guard isolate-period</b> | Sets the isolate time on the interface. |
|                  | <b>show nfpp dhcpv6-guard summary</b>   | Displays the configuration.             |

**Platform** N/A

**Description**

## 1.28 dhcpv6-guard monitored-host-limit

Use this command to set the maximum monitored host number. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard monitored-host-limit** *number*  
**no dhcpv6-guard monitored-host-limit**  
**default dhcpv6-guard monitored-host-limit**

| Parameter Description | Parameter     | Description                                                           |
|-----------------------|---------------|-----------------------------------------------------------------------|
|                       | <i>number</i> | The maximum monitored host number, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command Mode** NFPP configuration mode

**Usage Guide** If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message “%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.” to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts. to remind the administrator.

**Configuration Examples** The following example sets the maximum monitored host number to 200.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitored-host-limit 200

```

| Related Commands | Command                               | Description                 |
|------------------|---------------------------------------|-----------------------------|
|                  | <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration. |

**Platform Description** N/A

## 1.29 dhcpv6-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard monitor-period** *seconds*  
**no dhcpv6-guard monitor-period**  
**default dhcpv6-guard monitor-period**

| Parameter Description | Parameter      | Description                                                          |
|-----------------------|----------------|----------------------------------------------------------------------|
|                       | <i>seconds</i> | Sets the monitor time, in the range from 180 to 86400 in the unit of |

|  |          |
|--|----------|
|  | seconds. |
|--|----------|

**Defaults** The default is 600 seconds.

**Command Mode** NFPP configuration mode

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.  
If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration** The following example sets the monitor time to 180 seconds.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# dhcpv6-guard monitor-period 180

```

**Related Commands**

| Command                               | Description                       |
|---------------------------------------|-----------------------------------|
| <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.       |
| <b>show nfpp dhcpv6-guard hosts</b>   | Displays the monitored host list. |
| <b>clear nfpp dhcpv6-guard hosts</b>  | Clears the isolate host.          |

**Platform** N/A

**Description**

### 1.30 dhcpv6-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

```

dhcpv6-guard rate-limit { per-src-mac | per-port } pps
no dhcpv6-guard rate-limit { per-src-mac | per-port }
default dhcpv6-guard rate-limit { per-src-mac | per-port }

```

**Parameter Description**

| Parameter          | Description                                       |
|--------------------|---------------------------------------------------|
| <b>per-src-mac</b> | Sets the rate limit for each source MAC address.  |
| <b>per-port</b>    | Sets the rate limit for each port.                |
| <i>pps</i>         | Sets the rate limit, in the range from 1 to 9999. |

**Defaults** The default rate limit for each source MAC address is 5pps; the default rate limit for each port is 150pps.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the rate-limit threshold globally.

**Examples**

```

Hostname (config) # nfpp
Hostname (config-nfpp) # dhcpv6-guard rate-limit per-src-mac 8
Hostname (config-nfpp) # dhcpv6-guard rate-limit per-port 100

```

**Related  
Commands**

| Command                               | Description                                   |
|---------------------------------------|-----------------------------------------------|
| <b>nfpp dhcpv6-guard policy</b>       | Sets the rate limit and the attack threshold. |
| <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.                   |

**Platform** N/A

**Description**

## 1.31 dhcpv6-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**dhcpv6-guard trusted-host** *mac*

**no dhcpv6-guard trusted-host** { **all** | *mac* }

**default dhcpv6-guard trusted-host**

**Parameter  
Description**

| Parameter  | Description                |
|------------|----------------------------|
| <i>mac</i> | Sets the MAC address.      |
| <b>all</b> | Deletes all trusted hosts. |

**Defaults** N/A

**Command** NFPP configuration mode

**Mode**

**Usage Guide** After this function is enabled, the DHCPv6 packets are sent from the trusted host to CPU without rate limit or alarm notification.

Up to 500 trusted hosts are supported.

**Configuration** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

**Examples**

```

Hostname (config) # nfpp
Hostname (config-nfpp) # dhcpv6-guard trusted-host 0000.0000.1111

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A  
Description

## 1.32 icmp-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard attack-threshold** { per-src-ip | per-port } pps

**no icmp-guard attack-threshold** { per-src-ip | per-port }

**default icmp-guard attack-threshold** { per-src-ip | per-port }

| Parameter Description | Parameter       | Description                                                                              |
|-----------------------|-----------------|------------------------------------------------------------------------------------------|
|                       |                 | <b>per-src-ip</b>                                                                        |
|                       | <b>per-port</b> | Sets the attack threshold for each port.                                                 |
|                       | <i>pps</i>      | Sets the attack threshold, in the range from 1 to 9999 in the unit of <code>pps</code> . |

**Defaults** By default, the attack threshold for each source IP address is 200pps; and the attack threshold for each port is 400pps

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the global attack threshold.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Hostname(config-nfpp)# icmp-guard attack-threshold per-port 1200

```

| Related Commands | Command                             | Description                       |
|------------------|-------------------------------------|-----------------------------------|
|                  |                                     | <b>nfpp icmp-guard policy</b>     |
|                  | <b>show nfpp icmp-guard summary</b> | Displays the configuration.       |
|                  | <b>show nfpp icmp-guard hosts</b>   | Displays the monitored host list. |

|                                    |                            |
|------------------------------------|----------------------------|
| <b>clear nfpp icmp-guard hosts</b> | Clears the monitored host. |
|------------------------------------|----------------------------|

**Platform** N/A

**Description**

### 1.33 icmp-guard enable

Use this command to enable the ICMP anti-attack function. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard enable**

**no icmp-guard enable**

**default icmp-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the ICMP anti-attack function globally.

**Examples**

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard enable
```

| Related Commands | Command                             | Description                                             |
|------------------|-------------------------------------|---------------------------------------------------------|
|                  | <b>nfpp icmp-guard enable</b>       | Enables the ICMP anti-attack function on the interface. |
|                  | <b>show nfpp icmp-guard summary</b> | Displays the configuration.                             |

**Platform** N/A

**Description**

### 1.34 icmp-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard isolate-period** { *seconds* | **permanent** }

**no icmp-guard isolate-period**

**default icmp-guard isolate-period**

| Parameter Description | Parameter        | Description                                                                                       |
|-----------------------|------------------|---------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i>   | Sets the isolate time. The value is in the range is 0 or from 30 to 86400 in the unit of seconds. |
|                       | <b>permanent</b> | Permanent isolation.                                                                              |

**Defaults** The default is 0 second, which means no isolation.

**Command Mode** NFPP configuration mode

**Usage Guide** The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.

**Configuration** The following example sets the isolate time globally to 180 seconds.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard isolate-period 180
    
```

| Related Commands | Command                               | Description                             |
|------------------|---------------------------------------|-----------------------------------------|
|                  | <b>nfpp icmp-guard isolate-period</b> | Sets the isolate time on the interface. |
|                  | <b>show nfpp icmp-guard summary</b>   | Displays the configuration.             |

**Platform Description** N/A

### 1.35 icmp-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

- icmp-guard monitor-period** *seconds*
- no icmp-guard monitor-period**
- default icmp-guard monitor-period**

| Parameter Description | Parameter      | Description                                                    |
|-----------------------|----------------|----------------------------------------------------------------|
|                       | <i>seconds</i> | Sets the monitor time, in the range from 180 to 86400 seconds. |

**Defaults** The default is 600 seconds.

**Command** NFPP configuration mode



**Mode**

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.

**Configuration** The following example sets the monitor time to 180 seconds.

**Examples**

```
Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitor-period 180
```

**Related  
Commands**

| Command                             | Description                       |
|-------------------------------------|-----------------------------------|
| <b>show nfpp icmp-guard summary</b> | Displays the configuration.       |
| <b>show nfpp icmp-guard hosts</b>   | Displays the monitored host list. |
| <b>clear nfpp icmp-guard hosts</b>  | Clears the isolate host.          |

**Platform** N/A

**Description**

## 1.36 icmp-guard monitored-host-limit

Use this command to set the maximum monitored host number. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard monitored-host-limit** *number*

**no icmp-guard monitored-host-limit**

**default icmp-guard monitored-host-limit**

**Parameter  
Description**

| Parameter     | Description                                                           |
|---------------|-----------------------------------------------------------------------|
| <i>number</i> | The maximum monitored host number, in the range from 1 to 4294967295. |

**Defaults** The default is 1000.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** If the monitored host number has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts. to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum monitored host number has been exceeded, it prompts the message that %NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to remind the administrator.

**Configuration** The following example sets the maximum monitored host number to 200.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard monitored-host-limit 200

```

**Related Commands**

| Command                             | Description                 |
|-------------------------------------|-----------------------------|
| <b>show nfpp icmp-guard summary</b> | Displays the configuration. |

**Platform** N/A

**Description**

## 1.37 icmp-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard rate-limit { per-src-ip | per-port } pps**

**no icmp-guard rate-limit { per-src-ip | per-port }**

**default icmp-guard rate-limit { per-src-ip | per-port }**

**Parameter Description**

| Parameter         | Description                                       |
|-------------------|---------------------------------------------------|
| <b>per-src-ip</b> | Sets the rate limit for each source IP address.   |
| <b>per-port</b>   | Sets the rate limit for each port.                |
| <i>pps</i>        | Sets the rate limit, in the range from 1 to 9999. |

**Defaults** The default rate limit for each source IP address is 200 pps; the default rate limit for each port is 400pps.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the rate-limit threshold globally.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Hostname(config-nfpp)# icmp-guard rate-limit per-port 800

```

**Related Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                                     |                                               |
|-------------------------------------|-----------------------------------------------|
| <b>nfpp icmp-guard policy</b>       | Sets the rate limit and the attack threshold. |
| <b>show nfpp icmp-guard summary</b> | Displays the configuration.                   |

**Platform** N/A

**Description**

## 1.38 icmp-guard trusted-host

Use this command to set the trusted hosts free form monitoring. Use the **no** or **default** form of this command to restore the default setting.

**icmp-guard trusted-host** *ip mask*

**no icmp-guard trusted-host** { **all** | *ip mask* }

**default icmp-guard trusted-host**

| Parameter Description | Parameter   | Description                                     |
|-----------------------|-------------|-------------------------------------------------|
|                       | <i>ip</i>   | Sets the IP address.                            |
|                       | <i>mask</i> | Sets the IP mask.                               |
|                       | <b>all</b>  | Deletes the configuration of all trusted hosts. |

**Defaults** No trusted host is configured by default.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.

**Configuration** The following example sets the trusted hosts free form monitoring.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0

```

| Related Commands | Command                                  | Description                 |
|------------------|------------------------------------------|-----------------------------|
|                  | <b>show nfpp icmp-guard trusted-host</b> | Displays the configuration. |

**Platform** N/A

**Description**

## 1.39 ip-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard attack-threshold** { per-src-ip | per-port } pps

**no ip-guard attack-threshold** { per-src-ip | per-port }

**default ip-guard attack-threshold** { per-src-ip | per-port }

| Parameter Description | Parameter         | Description                                                      |
|-----------------------|-------------------|------------------------------------------------------------------|
|                       | <b>per-src-ip</b> | Sets the attack threshold for each source IP address.            |
|                       | <b>per-port</b>   | Sets the attack threshold for each port.                         |
|                       | <i>pps</i>        | Sets the attack threshold, in pps. The valid range is 1 to 9999. |

**Defaults** By default, the attack threshold for each source IP address and each port are 20pps and 2000pps respectively.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** The attack threshold shall be equal to or larger than the rate-limit threshold.

**Configuration** The following example sets the global attack threshold.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Hostname(config-nfpp)# ip-guard attack-threshold per-port 50

```

| Related Commands | Command                           | Description                                             |
|------------------|-----------------------------------|---------------------------------------------------------|
|                  | <b>nfpp ip-guard policy</b>       | Displays the rate-limit threshold and attack threshold. |
|                  | <b>show nfpp ip-guard summary</b> | Displays the configuration.                             |
|                  | <b>show nfpp ip-guard hosts</b>   | Displays the monitored host list.                       |
|                  | <b>clear nfpp ip-guard hosts</b>  | Clears the monitored host.                              |

**Platform** N/A

**Description**

## 1.40 ip-guard enable

Use this command to enable the IP anti-scan function. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard enable**  
**no ip-guard enable**  
**default ip-guard enable**

| Parameter<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          |           | N/A         |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables the IP anti-scan function globally.

```
Hostname(config)# nfp
Hostname(config-nfp)# ip-guard enable
```

| Related<br>Commands | Command | Description                |
|---------------------|---------|----------------------------|
|                     |         | <b>nfp ip-guard enable</b> |

**Platform Description** N/A

## 1.41 ip-guard isolate-period

Use this command to set the isolate time globally. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard isolate-period** { *seconds* | **permanent** }  
**no ip-guard isolate-period**  
**default ip-guard isolate-period**

| Parameter<br>Description | Parameter        | Description                                                                                    |
|--------------------------|------------------|------------------------------------------------------------------------------------------------|
|                          | <i>seconds</i>   | Sets the isolate time. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
|                          | <b>permanent</b> | Permanent isolation.                                                                           |

**Defaults** The default is 0 second, which means no isolation.

**Command** NFPP configuration mode

**Mode****Usage Guide** N/A**Configuration** The following example sets the isolate time globally to 180 seconds.**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard isolate-period 180

```

**Related  
Commands**

| Command                             | Description                             |
|-------------------------------------|-----------------------------------------|
| <b>nfpp ip-guard isolate-period</b> | Sets the isolate time on the interface. |
| <b>show nfpp ip-guard summary</b>   | Displays the configuration.             |

**Platform** N/A**Description**

## 1.42 ip-guard monitor-period

Use this command to configure the monitor time. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard monitor-period** *seconds***no ip-guard monitor-period****default ip-guard monitor-period****Parameter  
Description**

| Parameter      | Description                                                                   |
|----------------|-------------------------------------------------------------------------------|
| <i>seconds</i> | Sets the monitor time, in the range from 180 to 86400 in the unit of seconds. |

**Defaults** The default is 600 seconds.**Command** NFPP configuration mode**Mode**

**Usage Guide** When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0.

If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software

**Configuration** The following example sets the monitor time to 180 seconds.**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitor-period 180

```

| Related<br>Commands | Command                           | Description                       |
|---------------------|-----------------------------------|-----------------------------------|
|                     | <b>show nfpp ip-guard summary</b> | Displays the configuration.       |
|                     | <b>show nfpp ip-guard hosts</b>   | Displays the monitored host list. |
|                     | <b>clear nfpp ip-guard hosts</b>  | Clears the isolate host.          |

Platform N/A

Description

## 1.43 ip-guard monitored-host-limit

Use this command to set the maximum number of monitored hosts. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard monitored-host-limit** *number*

**no ip-guard monitored-host-limit**

**default ip-guard monitored-host-limit**

| Parameter<br>Description | Parameter     | Description |
|--------------------------|---------------|-------------|
|                          | <i>number</i> |             |

**Defaults** The default is 1000.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** If the number of monitored hosts has reached the default 1000, the administrator shall set the max-number smaller than 1000 and it will prompt the message “%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.” to remind the administrator of the invalid configuration and removing the monitored hosts.

When the maximum number of monitored hosts has been exceeded, it prompts the message that %NFPP\_ARP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of 1000 monitored hosts.to remind the administrator.

**Configuration** The following example sets the maximum number of monitored hosts to 200.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard monitored-host-limit 200

```

| Related<br>Commands | Command                           | Description                 |
|---------------------|-----------------------------------|-----------------------------|
|                     | <b>show nfpp ip-guard summary</b> | Displays the configuration. |

**Platform** N/A  
**Description**

## 1.44 ip-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

```
ip-guard rate-limit { per-src-ip | per-port } pps
no ip-guard rate-limit { per-src-ip | per-port }
default ip-guard rate-limit {per-src-ip | per-port }
```

| Parameter Description | Parameter         | Description                                     |
|-----------------------|-------------------|-------------------------------------------------|
|                       | <b>per-src-ip</b> | Sets the rate limit for each source IP address. |
|                       | <b>per-port</b>   | Sets the rate limit for each port.              |
|                       | <i>pps</i>        | Sets the rate limit, in the range of 1 to 9999. |

**Defaults** By default, the rate-limit threshold for each source IP address and each port is 20pps and 100pps respectively.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the rate-limit threshold globally.

```
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard rate-limit per-src-ip 2
Hostname(config-nfpp)# ip-guard rate-limit per-port 50
```

| Related Commands | Command                           | Description                                   |
|------------------|-----------------------------------|-----------------------------------------------|
|                  | <b>nfpp ip-guard policy</b>       | Sets the rate limit and the attack threshold. |
|                  | <b>show nfpp ip-guard summary</b> | Displays the configuration.                   |

**Platform** N/A  
**Description**

## 1.45 ip-guard scan-threshold

Use this command to set the global scan threshold. Use the **no** or **default** form of this command to restore the default setting.

```
ip-guard scan-threshold pkt-cnt
```



**no ip-guard scan-threshold**  
**default ip-guard scan-threshold**

**Parameter  
Description**

| Parameter      | Description                                           |
|----------------|-------------------------------------------------------|
| <i>pkt-cnt</i> | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** The default is 100 packets in 10 seconds.

**Command  
Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the global scan threshold to 20pps.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard scan-threshold 20

```

**Related  
Commands**

| Command                             | Description                          |
|-------------------------------------|--------------------------------------|
| <b>nfpp ip-guard scan-threshold</b> | Sets the scan threshold on the port. |
| <b>show nfpp ip-guard summary</b>   | Displays the configuration.          |

**Platform** N/A

**Description**

## 1.46 ip-guard trusted-host

Use this command to set the trusted host free form monitoring. Use the **no** or **default** form of this command to restore the default setting.

**ip-guard trusted-host** *ip mask*

**no ip-guard trusted-host** { **all** | *ip mask* }

**default ip-guard trusted-host**

**Parameter  
Description**

| Parameter   | Description                                     |
|-------------|-------------------------------------------------|
| <i>ip</i>   | Sets the IP address.                            |
| <i>mask</i> | Sets the IP mask.                               |
| <b>all</b>  | Deletes the configuration of all trusted hosts. |

**Defaults** N/A

**Command** NFPP configuration mode

**Mode**

**Usage Guide** The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to sent to the trusted host CPU without any rate-limit and warning. Configure the mask to set all hosts in one network segment free from monitoring. Up to 500 trusted hosts are supported.

**Configuration** The following example sets the trusted host free form monitoring.

```

Examples
Hostname(config)# nfpp
Hostname(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0
    
```

| Related Commands | Command | Description                            |
|------------------|---------|----------------------------------------|
|                  |         | <b>show nfpp ip-guard trusted-host</b> |

**Platform** N/A

**Description**

### 1.47 log-buffer entries

Use this command to set the size of the NFPP log buffer. Use the **no** or **default** form of this command to restore the default setting.

**log-buffer entries** *number*

**no log-buffer entries**

**default log-buffer entries**

| Parameter Description | Parameter | Description   |
|-----------------------|-----------|---------------|
|                       |           | <i>number</i> |

**Defaults** The default is 256.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the size of the NFPP log buffer.

```

Examples
Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer entries 50
    
```

| Related Commands | Command | Description                                              |
|------------------|---------|----------------------------------------------------------|
|                  |         | <b>log-buffer logs</b> <i>number-of-message interval</i> |

|                          |                                                        |
|--------------------------|--------------------------------------------------------|
| <i>length-in-seconds</i> | the NFPP buffer.                                       |
| <b>show nfpp log</b>     | Displays the NFPP log configuration or the log buffer. |

**Platform** N/A

**Description**

## 1.48 log-buffer logs

Use this command to set the rate of syslog generation from the NFPP log buffer. Use the **no** or **default** form of this command to restore the default setting.

**log-buffer logs** *number-of-message* **interval** *length-in-seconds*

**no log-buffer logs**

**default log-buffer logs**

| Parameter Description | Parameter                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>number-of-message</i> | The valid range is from 0 to 1024.<br>0 indicates that all logs are recorded in the specific buffer and no syslogs are generated.                                                                                                                                                                                                                                                                                                          |
|                       | <i>length-in-seconds</i> | The valid range is from 0 to 86400(one day).<br>0 indicates not to write the log to the buffer but generate the syslog immediately.<br>With both the <i>number-of-message</i> and <i>length-in-seconds</i> values are 0, it indicates not to write the log to the buffer but generate the syslog immediately.<br>The parameter <i>number-of-message /length-in-second</i> indicates the rate of syslog generated from the NFPP log buffer. |

**Defaults** By default, *number-of-message* is 1 and *length-in-seconds* is 30 seconds.

**Command** NFPP configuration mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example sets the rate of syslog generation from the NFPP log buffer.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# log-buffer logs 2 interval 12

```

| Related Commands | Command                                 | Description                                    |
|------------------|-----------------------------------------|------------------------------------------------|
|                  | <b>log-buffer entries</b> <i>number</i> | Sets the NFPP log buffer size.                 |
|                  | <b>show nfpp log summary</b>            | Displays the NFPP log configuration or the log |

|  |         |
|--|---------|
|  | buffer. |
|--|---------|

**Platform** N/A  
**Description**

## 1.49 logging

Run the **logging** command to configure NFPP to records the logs of a specified VLAN ID and a specified interface.. Use the **no** or **default** form of this command to restore the default setting.

- logging vlan** *vlan-range*
- logging interface** *interface-type interface-number*
- no logging vlan** *vlan-range*
- no logging interface** *interface-type interface-number*
- default logging**

| Parameter Description | Parameter                                        | Description                                                    |
|-----------------------|--------------------------------------------------|----------------------------------------------------------------|
|                       | <i>vlan-range</i>                                | Sets the specified VLAN range, in the format such as "1-3, 5". |
|                       | <i>interface-type</i><br><i>interface-number</i> | Sets the interface type and number.                            |

**Defaults** All logs are recorded by default.

**Command Mode** NFPP configuration mode

**Usage Guide** Use this command to filter the logs and records the logs within the specified VLAN range or the specified port

**Configuration Examples** The following example records the logs in VLAN 1, VLAN 2,VLAN 3 and VLAN 5 only.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# logging vlan 1-3,5
    
```

The following example records the logs on the interface GigabitEthernet 0/1 only.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# logging interface gigabitethernet 0/1
    
```

| Related Commands | Command                      | Description                                            |
|------------------|------------------------------|--------------------------------------------------------|
|                  | <b>show nfpp log summary</b> | Displays the NFPP log configuration or the log buffer. |

**Platform** N/A  
**Description**

## 1.50 nd-guard attack-threshold

Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the **no** or **default** form of this command to restore the default setting.

**nd-guard attack-threshold per-port { ns-na | rs | ra-redirect } pps**

**no nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }**

**default nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }**

| Parameter Description | Parameter          | Description                                                                    |
|-----------------------|--------------------|--------------------------------------------------------------------------------|
|                       | <b>ns-na</b>       | Sets the neighbor request and neighbor advertisement.                          |
|                       | <b>rs</b>          | Sets the router request.                                                       |
|                       | <b>ra-redirect</b> | Sets the router advertisement and the redirect packets.                        |
|                       | <i>pps</i>         | Sets the attack threshold, in the range from 1 to 9999 in the unit of seconds. |

**Defaults** 30pps

**Command Mode** NFPP configuration mode

**Usage Guide** The attack threshold shall be equal to or larger than the rate-limit threshold.

**Configuration Examples** The following example sets the global attack threshold.

```

Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Hostname(config-nfpp)# nd-guard attack-threshold per-port rs 10
Hostname(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10

```

| Related Commands | Command                           | Description                                             |
|------------------|-----------------------------------|---------------------------------------------------------|
|                  | <b>nfpp ip-guard policy</b>       | Displays the rate-limit threshold and attack threshold. |
|                  | <b>show nfpp ip-guard summary</b> | Displays the configuration.                             |

**Platform** N/A

**Description**

## 1.51 nd-guard enable

Use this command to enable ND anti-attack function. Use the **no** form of this command to disable ND anti-attack function. Use the **default** form of this command to restore the default setting.

**nd-guard enable**  
**no nd-guard enable**  
**default nd-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is enabled by default.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example enables ND anti-attack function.

```

Hostname (config) # nfpp
Hostname (config-nfpp) # nd-guard enable

```

| Related Commands | Command                           | Description                                       |
|------------------|-----------------------------------|---------------------------------------------------|
|                  | <b>nfpp nd-guard enable</b>       | Enables ND anti-attack function on the interface. |
|                  | <b>show nfpp nd-guard summary</b> | Displays the configuration.                       |

**Platform Description** N/A

## 1.52 nd-guard rate-limit

Use this command to set the rate-limit threshold globally. Use the **no** or **default** form of this command to restore the default setting.

```

nd-guard rate-limit per-port { ns-na | rs | ra-redirect } pps
no nd-guard rate-limit per-port { ns-na | rs | ra-redirect }
default nd-guard rate-limit per-port { ns-na | rs | ra-redirect }

```

| Parameter Description | Parameter          | Description                                                                   |
|-----------------------|--------------------|-------------------------------------------------------------------------------|
|                       | <b>ns-na</b>       | Sets the neighbor request and neighbor advertisement.                         |
|                       | <b>rs</b>          | Sets the router request.                                                      |
|                       | <b>ra-redirect</b> | Sets the router advertisement and the redirect packets.                       |
|                       | <i>pps</i>         | Sets the attack threshold, in the range is from 1 to 9999 in the unit of pps. |

**Defaults** 15 pps.

**Command Mode** NFPP configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the rate-limit threshold globally.

**Examples**

```

Hostname(config)# nfpp
Hostname(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Hostname(config-nfpp)# nd-guard rate-limit per-port rs 5
Hostname(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5

```

**Related Commands**

| Command                           | Description                                   |
|-----------------------------------|-----------------------------------------------|
| <b>nfpp nd-guard policy</b>       | Sets the rate limit and the attack threshold. |
| <b>show nfpp nd-guard summary</b> | Displays the configuration.                   |

**Platform** N/A

**Description**

## 1.53 nd-guard trusted-host

Use this command to set the trusted host. Use the **no** or **default** form of this command to restore the default setting.

**nd-guard trusted-host** *mac*

**no nd-guard trusted-host** { **all** | *mac* }

**default nd-guard trusted-host**

**Parameter Description**

| Parameter  | Description                |
|------------|----------------------------|
| <i>mac</i> | Sets the MAC address.      |
| <b>all</b> | Deletes all trusted hosts. |

**Defaults** N/A

**Command Mode** NFPP configuration mode

**Usage Guide** After this function is enabled, the ND packets are sent from the trusted host to CPU without rate limit or alarm notification.  
Up to 500 trusted hosts are supported.

**Configuration** The following example sets the host whose MAC address is 0000.0000.1111 as the trusted host.

**Examples**

```
Hostname(config)# nfpp
Hostname(config-nfpp)#nd-guard trusted-host 0000.0000.1111
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 1.54 nfpp arp-guard enable

Use this command to enable ARP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard enable**

**no nfpp arp-guard enable**

**default nfpp arp-guard enable**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

The ARP anti-attack function is not enabled on the interface.

**Command**

Interface configuration mode

**Mode****Usage Guide**

The interface ARP anti-attack configuration is prior to the global configuration.

**Configuration**

The following example enables ARP anti-attack function on the interface.

**Examples**

```
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp arp-guard enable
```

**Related  
Commands**

| Command                            | Description                       |
|------------------------------------|-----------------------------------|
| <b>arp-guard enable</b>            | Enables ARP anti-attack function. |
| <b>show nfpp arp-guard summary</b> | Displays the configuration.       |

**Platform**

N/A

**Description**



## 1.55 nfpp arp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp arp-guard isolate-period**

**default nfpp arp-guard isolate-period**

| Parameter Description | Parameter        | Description                                                                                       |
|-----------------------|------------------|---------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i>   | Sets the isolate period. The value is 0, or in the range from 30 to 86400 in the unit of seconds. |
|                       | <b>permanent</b> | Permanent isolation.                                                                              |

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the Interface configuration mode.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp arp-guard isolate-period 180

```

| Related Commands | Command                            | Description                     |
|------------------|------------------------------------|---------------------------------|
|                  | <b>arp-guard isolate-period</b>    | Sets the global isolate period. |
|                  | <b>show nfpp arp-guard summary</b> | Displays the configuration.     |

**Platform** N/A

**Description**

## 1.56 nfpp arp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** }

**default nfpp arp-guard policy** { **per-src-ip** | **per-src-mac** | **per-port** }

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|                             |                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------|
| <b>per-src-ip</b>           | Sets the rate-limit threshold and the attack threshold for each source IP address.  |
| <b>per-src-mac</b>          | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| <b>per-port</b>             | Sets the rate-limit threshold and the attack threshold for each port.               |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999.                         |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 9999.                             |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command** Interface configuration mode

**Mode**

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the local rate limiting threshold and local attack threshold of ARP guard to **50 pps** and **100 pps** for each interface on GigabitEthernet 0/1, to **2 pps** and **10 pps** for each source IP address, and to **3 pps** and **10 pps** for each source MAC address.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp arp-guard policy per-src-ip 2 10
Hostname(config-if)# nfpp arp-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp arp-guard policy per-port 50 100
    
```

**Related Commands**

| Command                            | Description                           |
|------------------------------------|---------------------------------------|
| <b>arp-guard attack-threshold</b>  | Sets the global attack threshold.     |
| <b>arp-guard rate-limit</b>        | Sets the global rate-limit threshold. |
| <b>show nfpp arp-guard summary</b> | Displays the configuration.           |
| <b>show nfpp arp-guard hosts</b>   | Displays the monitored host.          |
| <b>clear nfpp arp-guard hosts</b>  | Clears the isolate host.              |

**Platform** N/A

**Description**

### 1.57 nfpp arp-guard scan-threshold

Use this command to set the scan threshold. Use the **no** or **default** form of this command to restore the default setting.

- nfpp arp-guard scan-threshold** *pkt-cnt*
- no nfpp arp-guard scan-threshold**
- default nfpp arp-guard scan-threshold**

| Parameter Description | Parameter      | Description                                           |
|-----------------------|----------------|-------------------------------------------------------|
|                       | <i>pkt-cnt</i> | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** By default, the sport-based scan threshold is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the scan threshold to 20pps.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp arp-guard scan-threshold 20

```

| Related Commands | Command                            | Description                       |
|------------------|------------------------------------|-----------------------------------|
|                  | <b>arp-guard attack-threshold</b>  | Sets the global attack threshold. |
|                  | <b>show nfpp arp-guard summary</b> | Displays the configuration.       |
|                  | <b>show nfpp arp-guard scan</b>    | Displays the ARP scan table.      |
|                  | <b>clear nfpp arp-guard scan</b>   | Clears the ARP scan table.        |

**Platform** N/A

**Description**

## 1.58 nfpp dhcp-guard enable

Use this command to enable DHCP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard enable**

**no nfpp dhcp-guard enable**

**default nfpp dhcp-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The DHCP anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface DHCP anti- attack configuration is prior to the global configuration.

**Configuration** The following example enables DHCP anti-attack function on the interface.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcp-guard enable

```

**Related Commands**

| Command                             | Description                        |
|-------------------------------------|------------------------------------|
| <b>dhcp-guard enable</b>            | Enables DHCP anti-attack function. |
| <b>show nfpp dhcp-guard summary</b> | Displays the configuration.        |

**Platform**

N/A

**Description**

## 1.59 nfpp dhcp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp dhcp-guard isolate-period**

**default nfpp dhcp-guard isolate-period**

**Parameter Description**

| Parameter        | Description                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------|
| <i>seconds</i>   | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
| <b>permanent</b> | Permanent isolation.                                                                             |

**Defaults**

By default, the isolate period is not configured

**Command Mode**

Interface configuration mode

**Usage Guide**

N/A

**Configuration** The following example sets the isolate period to 180 seconds.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcp-guard isolate-period 180

```

**Related Commands**

| Command                             | Description                     |
|-------------------------------------|---------------------------------|
| <b>dhcp-guard isolate-period</b>    | Sets the global isolate period. |
| <b>show nfpp dhcp-guard summary</b> | Displays the configuration.     |

**Platform** N/A

**Description**

## 1.60 nfpp dhcp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcp-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp dhcp-guard policy** { **per-src-mac** | **per-port** }

**default nfpp dhcp-guard policy** { **per-src-mac** | **per-port** }

**Parameter Description**

| Parameter                   | Description                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------|
| <b>per-src-mac</b>          | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| <b>per-port</b>             | Sets the rate-limit threshold and the attack threshold for each port.               |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999.                         |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 9999.                             |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value should be no smaller than the rate-limit threshold.

**Configuration Examples** The following example sets the rate limiting threshold and attack threshold of DHCP guard to 50 pps and 100 pps for each interface on GigabitEthernet 0/1 and to 3 pps and 10 pps for each source MAC address.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcp-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp dhcp-guard policy per-port 50 100

```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.61 nfpp dhcpv6-guard enable

Use this command to enable the DHCPv6 anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard enable**

**no nfpp dhcpv6-guard enable**

**default nfpp dhcpv6-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The DHCPv6 anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface DHCPv6 anti- attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the DHCPv6 anti-attack function on interface gigabitethernet 0/1.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcpv6-guard enable

```

| Related Commands | Command                               | Description                           |
|------------------|---------------------------------------|---------------------------------------|
|                  | <b>dhcpv6-guard enable</b>            | Enables the ARP anti-attack function. |
|                  | <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.           |

**Platform Description** N/A

## 1.62 nfpp dhcpv6-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard isolate-period { *seconds* | permanent }**

**no nfpp dhcpv6-guard isolate-period**

**default nfpp dhcpv6-guard isolate-period**

| Parameter Description | Parameter      | Description                                                                                      |
|-----------------------|----------------|--------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |

|                  |                      |
|------------------|----------------------|
| <b>permanent</b> | Permanent isolation. |
|------------------|----------------------|

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the interface configuration mode to 180 seconds.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcpv6-guard isolate-period 180

```

**Related Commands**

| Command                               | Description                     |
|---------------------------------------|---------------------------------|
| <b>dhcpv6-guard isolate-period</b>    | Sets the global isolate period. |
| <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.     |

**Platform Description** N/A

## 1.63 nfpp dhcpv6-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp dhcpv6-guard policy { per-src-mac | per-port } rate-limit-pps attack-threshold-pps**

**no nfpp dhcpv6-guard policy { per-src-mac | per-port }**

**default nfpp dhcpv6-guard policy { per-src-mac | per-port }**

**Parameter Description**

| Parameter                   | Description                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------|
| <b>per-src-mac</b>          | Sets the rate-limit threshold and the attack threshold for each source MAC address. |
| <b>per-port</b>             | Sets the rate-limit threshold and the attack threshold for each port.               |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999.                         |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 9999.                             |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value should be no smaller than the rate-limit threshold.

**Configuration Examples** The following example sets the rate-limit threshold and the attack threshold for DHCP attack defense on GigabitEthernet 0/1. The IP-based rate-limit threshold is set to 2 pps and the attack threshold is set to 10 pps; the MAC address-based rate-limit threshold is set to 3 pps and the attack threshold is set to 10 pps; the interface-based rate-limit threshold is set to 50 pps and the attack threshold is set to 100 pps.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Hostname(config-if)# nfpp dhcpv6-guard policy per-port 50 100
    
```

**Related Commands**

| Command                               | Description                           |
|---------------------------------------|---------------------------------------|
| <b>dhcpv6-guard attack-threshold</b>  | Sets the global attack threshold.     |
| <b>dhcpv6-guard rate-limit</b>        | Sets the global rate-limit threshold. |
| <b>show nfpp dhcpv6-guard summary</b> | Displays the configuration.           |
| <b>show nfpp dhcpv6-guard hosts</b>   | Displays the monitored host.          |
| <b>clear nfpp dhcpv6-guard hosts</b>  | Clears the isolate host.              |

**Platform** N/A

**Description**

## 1.64 nfpp icmp-guard enable

Use this command to enable the ICMP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

- nfpp icmp-guard enable**
- no nfpp icmp-guard enable**
- default nfpp icmp-guard enable**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** The ICMP anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface ICMP anti- attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ICMP anti-attack function on the interface.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp icmp-guard enable
    
```



| Related<br>Commands | Command                             | Description                           |
|---------------------|-------------------------------------|---------------------------------------|
|                     | <b>icmp-guard enable</b>            | Enables the ARP anti-attack function. |
|                     | <b>show nfpp icmp-guard summary</b> | Displays the configuration.           |

Platform N/A  
Description

## 1.65 nfpp icmp-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp icmp-guard isolate-period** { *seconds* | **permanent** }

**no nfpp icmp-guard isolate-period**

**default nfpp icmp-guard isolate-period**

| Parameter<br>Description | Parameter        | Description                                                                                      |
|--------------------------|------------------|--------------------------------------------------------------------------------------------------|
|                          | <i>seconds</i>   | Sets the isolate period. The value is 0 or in the range from 30 to 86400 in the unit of seconds. |
|                          | <b>permanent</b> | Permanent isolation.                                                                             |

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the isolate period in the interface configuration mode.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp icmp-guard isolate-period 180

```

| Related<br>Commands | Command                             | Description                     |
|---------------------|-------------------------------------|---------------------------------|
|                     | <b>icmp-guard isolate-period</b>    | Sets the global isolate period. |
|                     | <b>show nfpp icmp-guard summary</b> | Displays the configuration.     |

Platform N/A  
Description

## 1.66 nfpp icmp-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp icmp-guard policy** { **per-src-ip** | **per-port** } *rate-limit-pps attack-threshold-pps*

**no nfpp icmp-guard policy** { **per-src-ip** | **per-port** }

**default nfpp icmp-guard policy** { **per-src-ip** | **per-port** }

| Parameter Description | Parameter                   | Description                                                                        |
|-----------------------|-----------------------------|------------------------------------------------------------------------------------|
|                       | <b>per-src-ip</b>           | Sets the rate-limit threshold and the attack threshold for each source IP address. |
|                       | <b>per-port</b>             | Sets the rate-limit threshold and the attack threshold for each port.              |
|                       | <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999.                        |
|                       | <i>attack-threshold-pps</i> | Sets the attack threshold, in range from 1 to 9999.                                |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the rate limiting threshold and attack threshold of ICMP guard to **100** pps and 200 pps for each interface on GigabitEthernet 0/1 and to 5 pps and 10 pps for each source IP address.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Hostname(config-if)# nfpp icmp-guard policy per-port 100 200

```

| Related Commands | Command                             | Description                           |
|------------------|-------------------------------------|---------------------------------------|
|                  | <b>icmp-guard attack-threshold</b>  | Sets the global attack threshold.     |
|                  | <b>icmp-guard rate-limit</b>        | Sets the global rate-limit threshold. |
|                  | <b>show nfpp icmp-guard summary</b> | Displays the configuration.           |
|                  | <b>show nfpp icmp-guard hosts</b>   | Displays the monitored host.          |
|                  | <b>clear nfpp icmp-guard hosts</b>  | Clears the isolate host.              |

**Platform Description** N/A

## 1.67 nfpp ip-guard enable

Use this command to enable the ICMP anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard enable**

**no nfpp ip-guard enable**

**default nfpp ip-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The IP anti-scan function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface IP anti-scan configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ICMP anti-attack function on the interface.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp ip-guard enable

```

| Related Commands | Command                           | Description                           |
|------------------|-----------------------------------|---------------------------------------|
|                  | <b>ip-guard enable</b>            | Enables the ARP anti-attack function. |
|                  | <b>show nfpp ip-guard summary</b> | Displays the configuration.           |

**Platform** N/A

**Description**

## 1.68 nfpp ip-guard isolate-period

Use this command to set the isolate period in the interface configuration mode. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard isolate-period** { *seconds* | **permanent** }

**no nfpp ip-guard isolate-period**

**default nfpp ip-guard isolate-period**

| Parameter Description | Parameter      | Description                                                                    |
|-----------------------|----------------|--------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Sets the isolate period, in the range from 30 to 86400 in the unit of seconds. |

|                  |                      |
|------------------|----------------------|
| <b>permanent</b> | Permanent isolation. |
|------------------|----------------------|

**Defaults** By default, the isolate period is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration** The following example sets the isolate period in the interface configuration mode.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp ip-guard isolate-period 180

```

**Related Commands**

| Command                           | Description                     |
|-----------------------------------|---------------------------------|
| <b>ip-guard isolate-period</b>    | Sets the global isolate period. |
| <b>show nfpp ip-guard summary</b> | Displays the configuration.     |

**Platform** N/A

**Description**

## 1.69 nfpp ip-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard policy { per-src-ip | per-port } rate-limit-pps attack-threshold-pps**

**no nfpp ip-guard policy { per-src-ip | per-port }**

**default nfpp ip-guard policy { per-src-ip | per-port }**

**Parameter Description**

| Parameter                   | Description                                                                        |
|-----------------------------|------------------------------------------------------------------------------------|
| <b>per-src-ip</b>           | Sets the rate-limit threshold and the attack threshold for each source IP address. |
| <b>per-port</b>             | Sets the rate-limit threshold and the attack threshold for each port.              |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999.                        |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 9999.                            |

**Defaults** By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command Mode** Interface configuration mode

**Usage Guide** The attack threshold value shall be equal to or greater than the rate-limit threshold.

**Configuration Examples** The following example sets the rate limiting threshold and attack threshold of IP guard to 50 pps and 100 pps for each interface on GigabitEthernet 0/1 and to 2 pps and 10 pps for each source IP address.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp ip-guard policy per-src-ip 2 10
Hostname(config-if)# nfpp ip-guard policy per-port 50 100
    
```

**Related Commands**

| Command                           | Description                           |
|-----------------------------------|---------------------------------------|
| <b>ip-guard attack-threshold</b>  | Sets the global attack threshold.     |
| <b>ip-guard rate-limit</b>        | Sets the global rate-limit threshold. |
| <b>show nfpp ip-guard summary</b> | Displays the configuration.           |
| <b>show nfpp ip-guard hosts</b>   | Displays the monitored host.          |
| <b>clear nfpp ip-guard hosts</b>  | Clears the isolate host.              |

**Platform** N/A

**Description**

## 1.70 nfpp ip-guard scan-threshold

Use this command to set the scan threshold. Use the **no** or **default** form of this command to restore the default setting.

**nfpp ip-guard scan-threshold** *pkt-cnt*  
**no nfpp ip-guard scan-threshold**  
**default nfpp ip-guard scan-threshold**

**Parameter Description**

| Parameter      | Description                                           |
|----------------|-------------------------------------------------------|
| <i>pkt-cnt</i> | Sets the scan threshold, in the range from 1 to 9999. |

**Defaults** By default, the sport-based scan threshold is not configured.

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the scan threshold to 20pps.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp ip-guard scan-threshold 20
    
```

| Related Commands | Command                           | Description                       |
|------------------|-----------------------------------|-----------------------------------|
|                  | <b>ip-guard attack-threshold</b>  | Sets the global attack threshold. |
|                  | <b>show nfpp ip-guard summary</b> | Displays the configuration.       |

Platform N/A

Description

## 1.71 nfpp nd-guard enable

Use this command to enable the ND anti-attack function on the interface. Use the **no** or **default** form of this command to restore the default setting.

**nfpp nd-guard enable**

**no nfpp nd-guard enable**

**default nfpp nd-guard enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The ND anti-attack function is not enabled on the interface.

**Command Mode** Interface configuration mode

**Usage Guide** The interface ND anti-attack configuration is prior to the global configuration.

**Configuration Examples** The following example enables the ND anti-attack function on the interface.

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp nd-guard enable

```

| Related Commands | Command                           | Description                          |
|------------------|-----------------------------------|--------------------------------------|
|                  | <b>nd-guard enable</b>            | Enables the ND anti-attack function. |
|                  | <b>show nfpp nd-guard summary</b> | Displays the configuration.          |

Platform N/A

Description

## 1.72 nfpp nd-guard policy

Use this command to set the rate-limit threshold and the attack threshold. Use the **no** or **default** form of this command to restore the default setting.

```

nfpp nd-guard policy per-port { ns-na | rs | ra-redirect } rate-limit-pps attack-threshold-pps
no nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }
default nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }

```

**Parameter  
Description**

| Parameter                   | Description                                                 |
|-----------------------------|-------------------------------------------------------------|
| <b>ns-na</b>                | Sets the neighbor request and neighbor advertisement.       |
| <b>rs</b>                   | Sets the router request.                                    |
| <b>ra-redirect</b>          | Sets the router advertisement and the redirect packets.     |
| <i>rate-limit-pps</i>       | Sets the rate-limit threshold, in the range from 1 to 9999. |
| <i>attack-threshold-pps</i> | Sets the attack threshold, in the range from 1 to 9999.     |

**Defaults**

By default, the rate-limit threshold and the attack threshold are not configured. The global rate-limit threshold and the attack threshold are used.

**Command**

Interface configuration mode

**Mode**

**Usage Guide**

The attack threshold value shall be equal to or greater than the rate-limit threshold. For ND snooping, the port is classified into untrusted port and trusted port. The untrusted port connects to the host and the trusted port connects to the gateway. The rate-limit threshold for the trusted port shall higher than the one for the untrusted port because the traffic of the trusted port generally is higher than the traffic of the untrusted port. For the trusted port with ND snooping enabled, ND snooping advertises ND guard to set the rate-limit threshold and attack threshold for the three categories of packets as 800pps and 900pps respectively.

**Configuration**

The following example sets the rate-limit threshold and the attack threshold for ND attack defense on GigabitEthernet 0/1. The interface-based NS-NA rate-limit threshold is set to 50 pps and the attack threshold is set to 100 pps; the interface-based RS rate-limit threshold is set to 10 pps and the attack threshold is set to 20 pps; the interface-based RA-Direct rate-limit threshold is set to 10 pps and the attack threshold is set to 20 pps.

**Examples**

```

Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Hostname(config-if)# nfpp nd-guard policy per-port rs 10 20
Hostname(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20

```

**Related  
Commands**

| Command                           | Description                           |
|-----------------------------------|---------------------------------------|
| <b>nd-guard attack-threshold</b>  | Sets the global attack threshold.     |
| <b>nd-guard rate-limit</b>        | Sets the global rate-limit threshold. |
| <b>show nfpp nd-guard summary</b> | Displays the configuration.           |

**Platform**

N/A

**Description**

## 1.73 show nfpp arp-guard hosts

Use this command to display the monitored host.

```
show nfpp arp-guard hosts [ statistics | [ [ vlan vid ] [ interface interface-type interface-number ]
[ ip-address | mac-address ] ] ]
```

| Parameter Description | Parameter                          | Description                                                 |
|-----------------------|------------------------------------|-------------------------------------------------------------|
|                       | statistics                         | Displays the statistical information of the monitored host. |
|                       | vid                                | The VLAN ID.                                                |
|                       | interface-type<br>interface-number | The interface type and number.                              |
|                       | ip-address                         | The IP address.                                             |
|                       | mac-address                        | The MAC address.                                            |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the statistical information of the monitored host.

```
Examples
Hostname# show nfpp arp-guard hosts statistics
success    fail    total
-----    ----    -----
100        20     120
```

The following example shows the monitored host:

```
Hostname# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user".
VLAN interface IP address MAC address remain-time(s)
---- -
1 Gi0/1 1.1.1.1 - 110
2 Gi0/2 1.1.2.1 - 61
*3 Gi0/3 - 0000.0000.1111 110
4 Gi0/4 - 0000.0000.2222 61
Total:4 hosts
```

| Related Commands | Command                    | Description                |
|------------------|----------------------------|----------------------------|
|                  | clear nfpp arp-guard hosts | Clears the monitored host. |

**Platform** N/A



## Description

## 1.74 show nfpp arp-guard scan

Use this command to display the ARP scan list.

```
show nfpp arp-guard scan [ statistics ] [ [ vlan vid ] [ interface interface-type interface-number ]
[ mac-address ] ] ]
```

| Parameter Description | Parameter                                        | Description                                                |
|-----------------------|--------------------------------------------------|------------------------------------------------------------|
|                       | <b>statistics</b>                                | Displays the statistical information of the ARP scan list. |
|                       | <i>vid</i>                                       | The VLAN ID.                                               |
|                       | <i>interface-type</i><br><i>interface-number</i> | The interface type and interface number.                   |
|                       | <i>mac-address</i>                               | The MAC address.                                           |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the ARP scan statistics.

```
Hostname# show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).
```

The following example displays the ARP scan list.

```
Hostname# show nfpp arp-guard scan
VLAN   interface  IP address  MAC address  timestamp
----   -
1      Gi0/1     N/A        0000.0000.0001  2008-01-23 16:23:10
2      Gi0/2     1.1.1.1    0000.0000.0002  2008-01-23 16:24:10
3      Gi0/3     N/A        0000.0000.0003  2008-01-23 16:25:10
4      Gi0/4     N/A        0000.0000.0004  2008-01-23 16:26:10
Total:4 record(s)
```

The following example displays the ARP scan for VLAN 1.

```
Hostname# show nfpp arp-guard scan vlan 1 interface gigabitethernet 0/1
0000.0000.0001
VLAN   interface  IP address  MAC address  timestamp
----   -
1      Gi0/1     N/A        0000.0000.0001  2008-01-23 16:23:10
Total:1 record(s)
```

| Related Commands | Command                       | Description                     |
|------------------|-------------------------------|---------------------------------|
|                  | arp-guard scan-threshold      | Sets the global scan threshold. |
|                  | nfpp arp-guard scan-threshold | Sets the scan threshold.        |
|                  | clear nfpp arp-guard scan     | Clears the ARP scan list.       |

Platform N/A

Description

## 1.75 show nfpp arp-guard summary

Use this command to display the configuration.

**show nfpp arp-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

Configuration The following example displays the configuration.

```

Examples
Hostname# show nfpp arp-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300           4/5/60    8/10/100    15
Gi 0/1      Enable  180           5/-/-    8/-/-      -
Gi 0/2      Disable 200           4/5/60    8/10/100    20

Maximum count of monitored hosts: 1000
Monitor period:300s
    
```

| Field             | Description                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration mode.                                                                                                |
| Status            | Enables/Disables the anti-attack function.                                                                                |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ |

|                  |                                       |
|------------------|---------------------------------------|
|                  | the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| -                | No configuration.                     |

**Related Commands**

| Command                               | Description                                            |
|---------------------------------------|--------------------------------------------------------|
| <b>arp-guard attack-threshold</b>     | Sets the global attack threshold.                      |
| <b>arp-guard enable</b>               | Enables the ARP anti-attack function.                  |
| <b>arp-guard isolate-period</b>       | Sets the global isolate time.                          |
| <b>arp-guard monitor-period</b>       | Sets the monitor period.                               |
| <b>arp-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.        |
| <b>arp-guard rate-limit</b>           | Sets the global rate-limit threshold.                  |
| <b>arp-guard scan-threshold</b>       | Sets the global scan threshold.                        |
| <b>nfpp arp-guard enable</b>          | Enables the ARP anti-attack function on the interface. |
| <b>nfpp arp-guard isolate-period</b>  | Sets the isolate time.                                 |
| <b>nfpp arp-guard policy</b>          | Sets the rate-limit threshold and attack threshold.    |
| <b>nfpp arp-guard scan-threshold</b>  | Sets the scan threshold.                               |

**Platform** N/A  
**Description**

### 1.76 show nfpp arp-guard trusted-host

Use this command to display the trusted host.

**show nfpp arp-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the trusted host.

**Examples**

```

Hostname# show nfpp arp-guard trusted-host
IP address      mac
    
```

```

-----
1.1.1.1      0000.0000.1111
1.1.2.1      0000.0000.2222
Total: 2 record(s)
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

### 1.77 show nfpp dhcp-guard hosts

Use this command to display the monitored host.

**show nfpp dhcp-guard hosts** [ **statistics** | [ [ **vlan** *vid* ] [ **interface** *interface-type interface-number* ] [ *mac-address* ] ] ]

| Parameter Description | Parameter                                        | Description                                                 |
|-----------------------|--------------------------------------------------|-------------------------------------------------------------|
|                       | <b>statistics</b>                                | Displays the statistical information of the monitored host. |
|                       | <i>vid</i>                                       | The VLAN ID.                                                |
|                       | <i>interface-type</i><br><i>interface-number</i> | The interface type and number.                              |
|                       | <i>mac-address</i>                               | The MAC address.                                            |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```

Hostname# show nfpp dhcp-guard hosts statistics
success  fail  total
-----  ---  -----
100      20   120
    
```

The following example shows the monitored host:

```

Hostname# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface  MAC address  remain-time(seconds)
----  -
    
```

```

1    gi0/2    0000.0000.0001  10
*2  gi0/1    0000.0000.0002  20
Total:2 host(s)
    
```

| Related Commands | Command | Description                        |
|------------------|---------|------------------------------------|
|                  |         | <b>clear nfpp dhcp-guard hosts</b> |

**Platform** N/A  
**Description**

### 1.78 show nfpp dhcp-guard summary

Use this command to display the configuration.

**show nfpp dhcp-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the configuration.

```

Hostname# show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period  Rate-limit  Attack-threshold
Global     Enable  300             -/5/150    -/10/300
Gi 0/1     Enable  180             -/6/-      -/8/-
Gi 0/2     Disable 200             -/5/30     -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
    
```

| Field             | Description                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration mode.                                                                                                |
| Status            | Enables/Disables the anti-attack function.                                                                                |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ |

|                  |                                       |
|------------------|---------------------------------------|
|                  | the rate-limit threshold for the port |
| Attack-threshold | In the same format as the rate-limit. |
| -                | No configuration.                     |

**Related Commands**

| Command                                | Description                                             |
|----------------------------------------|---------------------------------------------------------|
| <b>dhcp-guard attack-threshold</b>     | Sets the global attack threshold.                       |
| <b>dhcp-guard enable</b>               | Enables the DHCP anti-attack function.                  |
| <b>dhcp-guard isolate-period</b>       | Sets the global isolate time.                           |
| <b>dhcp-guard monitor-period</b>       | Sets the monitor period.                                |
| <b>dhcp-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.         |
| <b>dhcp-guard rate-limit</b>           | Sets the global rate-limit threshold.                   |
| <b>nfpp dhcp-guard enable</b>          | Enables the DHCP anti-attack function on the interface. |
| <b>nfpp dhcp-guard isolate-period</b>  | Sets the isolate time.                                  |
| <b>nfpp dhcp-guard policy</b>          | Sets the rate-limit threshold and attack threshold.     |

**Platform** N/A

**Description**

## 1.79 show nfpp dhcp-guard trusted-host

Use this command to display the trusted host.

**show nfpp dhcp-guard trusted-host**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the trusted host.

```

Hostname# show nfpp dhcp-guard trusted-host
mac
-----
0000.0000.1111
    
```

```
0000.0000.2222
Total: 2 record(s)
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.80 show nfpp dhcpv6-guard hosts

Use this command to display the monitored host.

**show nfpp dhcpv6-guard hosts** [ **statistics** ] [ [ *vlan vid* ] [ **interface** *interface-type interface-number* ] [ *mac-address* ] ]

**Parameter Description**

| Parameter                              | Description                                                 |
|----------------------------------------|-------------------------------------------------------------|
| <b>statistics</b>                      | Displays the statistical information of the monitored host. |
| <i>vid</i>                             | The VLAN ID.                                                |
| <i>interface-type interface-number</i> | The interface type and number.                              |
| <i>mac-address</i>                     | The MAC address.                                            |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```
Hostname# show nfpp dhcpv6-guard hosts statistics
success  fail   total
-----  ----  -----
100      20    120
```

The following example shows the monitored host:

```
Hostname# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN interface  MAC address  remain-time(seconds)
----  -
1     gi0/2      0000.0000.0001  10
*2    gi0/1      0000.0000.0002  20
```

```
Total:2 host(s)
```

| Related Commands | Command | Description                                |
|------------------|---------|--------------------------------------------|
|                  |         | <code>clear nfpp dhcpv6-guard hosts</code> |

Platform N/A

Description

## 1.81 show nfpp dhcpv6-guard summary

Use this command to display the configuration.

**show nfpp dhcpv6-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           | N/A         |

Defaults N/A

Command Privileged EXEC mode  
Mode

Usage Guide N/A

Configuration The following example displays the configuration.

```
Examples
Hostname# show nfpp dhcpv6-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global Enable 300 -/5/150 -/10/300
Gi 0/1 Enable 180 -/6/- -/8/-
Gi 0/2 Disable 200 -/5/30 -/10/50

Maximum count of monitored hosts: 1000
Monitor period:300s
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |



|                  |                                       |
|------------------|---------------------------------------|
| Attack-threshold | In the same format as the rate-limit. |
| -                | No configuration.                     |

**Related Commands**

| Command                                  | Description                                               |
|------------------------------------------|-----------------------------------------------------------|
| <b>dhcpv6-guard attack-threshold</b>     | Sets the global attack threshold.                         |
| <b>dhcpv6-guard enable</b>               | Enables the DHCPv6 anti-attack function.                  |
| <b>dhcpv6-guard isolate-period</b>       | Sets the global isolate time.                             |
| <b>dhcpv6-guard monitor-period</b>       | Sets the monitor period.                                  |
| <b>dhcpv6-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.           |
| <b>dhcpv6-guard rate-limit</b>           | Sets the global rate-limit threshold.                     |
| <b>nfpp dhcpv6-guard enable</b>          | Enables the DHCPv6 anti-attack function on the interface. |
| <b>nfpp dhcpv6-guard isolate-period</b>  | Sets the isolate time.                                    |
| <b>nfpp dhcpv6-guard policy</b>          | Sets the rate-limit threshold and attack threshold.       |

**Platform** N/A

**Description**

## 1.82 show nfpp dhcpv6-guard trusted-host

Use this command to display the trusted host.

**show nfpp dhcpv6-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the trusted host.

**Examples**

```

Hostname# show nfpp dhcpv6-guard trusted-host
mac
-----
0000.0000.1111
0000.0000.2222
    
```

Total: 2 record(s)

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A

Description

### 1.83 show nfpp icmp-guard hosts

Use this command to display the monitored host.

**show nfpp icmp-guard hosts** [ **statistics** | [ [ *vlan vid* ] [ **interface** *interface-type interface-number* ] [ *ip-address* ] ] ]

| Parameter Description                            | Parameter         | Description                    |
|--------------------------------------------------|-------------------|--------------------------------|
|                                                  | <b>statistics</b> |                                |
| <i>vid</i>                                       |                   | The VLAN ID.                   |
| <i>interface-type</i><br><i>interface-number</i> |                   | The interface type and number. |
| <i>ip-address</i>                                |                   | The IP address.                |

Defaults N/A

Command Privileged EXEC mode  
Mode

Usage Guide N/A

Configuration The following example displays the statistical information of the monitored host.

```

Examples
Hostname# show nfpp icmp-guard hosts statistics
success    fail    total
-----    ----    -----
100        20     120
    
```

The following example displays the monitored host.

```

Hostname# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface IP address      remain-time(s)
----  -
1     Gi0/1      1.1.1.1      110
2     Gi0/2      1.1.2.1      61
Total:2 host(s)
    
```

| Related Commands | Command | Description                              |
|------------------|---------|------------------------------------------|
|                  |         | <code>clear nfpp icmp-guard hosts</code> |

**Platform** N/A  
**Description**

## 1.84 show nfpp icmp-guard summary

Use this command to display the configuration.

**show nfpp icmp-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

```

Examples
Hostname# show nfpp icmp-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period  Rate-limit  Attack-threshold
Global      Enable  300              4/-/60     8/-/100
Gi 0/1      Enable  180              5/-/-      8/-/-
Gi 0/2      Disable 200              4/-/60     8/-/100

Maximum count of monitored hosts: 1000
Monitor period:300s
    
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration mode.                                                                                                                                      |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |

|   |                   |
|---|-------------------|
| - | No configuration. |
|---|-------------------|

**Related Commands**

| Command                                | Description                                             |
|----------------------------------------|---------------------------------------------------------|
| <b>icmp-guard attack-threshold</b>     | Sets the global attack threshold.                       |
| <b>icmp-guard enable</b>               | Enables the ICMP anti-attack function.                  |
| <b>icmp-guard isolate-period</b>       | Sets the global isolate time.                           |
| <b>icmp-guard monitor-period</b>       | Sets the monitor period.                                |
| <b>icmp-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.         |
| <b>icmp-guard rate-limit</b>           | Sets the global rate-limit threshold.                   |
| <b>nfpp icmp-guard enable</b>          | Enables the ICMP anti-attack function on the interface. |
| <b>nfpp icmp-guard isolate-period</b>  | Sets the isolate time.                                  |
| <b>nfpp icmp-guard policy</b>          | Sets the rate-limit threshold and attack threshold.     |

**Platform** N/A

**Description**

## 1.85 show nfpp icmp-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp icmp-guard summary**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the trusted host free from being monitored.

**Examples**

```

Hostname# show nfpp icmp-guard trusted-host
IP address      mask
-----
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total:2 record(s)
    
```

| Related Commands | Command | Description                    |
|------------------|---------|--------------------------------|
|                  |         | <b>icmp-guard trusted-host</b> |

**Platform** N/A

**Description**

## 1.86 show nfpp ip-guard hosts

Use this command to display the monitored host.

**show nfpp ip-guard hosts** [ **statistics** | [ [ **vlan** *vid* ] [ **Interface** *interface-type interface-number* ] [ *ip-address* ] ] ]

| Parameter Description | Parameter                                        | Description                    |
|-----------------------|--------------------------------------------------|--------------------------------|
|                       |                                                  | <b>statistics</b>              |
|                       | <i>vid</i>                                       | The VLAN ID.                   |
|                       | <i>interface-type</i><br><i>interface-number</i> | The interface type and number. |
|                       | <i>ip-address</i>                                | The IP address.                |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays the statistical information of the monitored host.

```

Hostname# show nfpp ip-guard hosts statistics
success    fail    total
-----    ----    -----
100        20     120

```

The following example displays the monitored host for the IP anti-attack.

```

Hostname#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface IP address  Reason    remain-time(s)
----  -
1     Gi0/1    1.1.1.1   ATTACK    110
2     Gi0/2    1.1.2.1   SCAN      61
Total:2 host(s)

```

| Related Commands | Command | Description                            |
|------------------|---------|----------------------------------------|
|                  |         | <code>clear nfpp ip-guard hosts</code> |

**Platform** N/A  
**Description**

## 1.87 show nfpp ip-guard summary

Use this command to display the configuration.

**show nfpp ip-guard summary**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

```

Examples
Hostname# show nfpp ip-guard summary
(Format of column Rate-limit and Attack-threshold is
per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global Enable 300 4-/60 8-/100 15
Gi 0/1 Enable 180 5/-/- 8/-/- -
Gi 0/2 Disable 200 4-/60 8-/100 20

Maximum count of monitored hosts: 1000
Monitor period..300s
    
```

| Field             | Description                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface(Global) | Global configuration                                                                                                                                            |
| Status            | Enables/Disables the anti-attack function.                                                                                                                      |
| Rate-limit        | In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port |
| Attack-threshold  | In the same format as the rate-limit.                                                                                                                           |
| -                 | No configuration.                                                                                                                                               |

| Related<br>Commands | Command                              | Description                                         |
|---------------------|--------------------------------------|-----------------------------------------------------|
|                     | <b>ip-guard attack-threshold</b>     | Sets the global attack threshold.                   |
|                     | <b>ip-guard enable</b>               | Enables the IP anti-scan function.                  |
|                     | <b>ip-guard isolate-period</b>       | Sets the global isolate time.                       |
|                     | <b>ip-guard monitor-period</b>       | Sets the monitor period.                            |
|                     | <b>ip-guard monitored-host-limit</b> | Sets the maximum number of the monitored hosts.     |
|                     | <b>ip-guard rate-limit</b>           | Sets the global rate-limit threshold.               |
|                     | <b>nfpp ip-guard enable</b>          | Enables the IP anti-scan function on the interface. |
|                     | <b>nfpp ip-guard isolate-period</b>  | Sets the isolate time.                              |
|                     | <b>nfpp ip-guard policy</b>          | Sets the rate-limit threshold and attack threshold. |

**Platform** N/A

**Description**

## 1.88 show nfpp ip-guard trusted-host

Use this command to display the trusted host free from being monitored.

**show nfpp ip-guard summary**

| Parameter<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          | N/A       | N/A         |

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the trusted host free from being monitored.

```

Examples
Hostname# show nfpp ip-guard trusted-host
IP address      mask
-----
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total.2 record(s)

```

| Related Commands | Command | Description                        |
|------------------|---------|------------------------------------|
|                  |         | <code>ip-guard trusted-host</code> |

**Platform** N/A

**Description**

## 1.89 show nfpp log

Use this command to display the NFPP log configuration.

**show nfpp log summary**

Use this command to display the NFPP log buffer content.

**show nfpp log buffer [ statistics ]**

| Parameter Description | Parameter | Description             |
|-----------------------|-----------|-------------------------|
|                       |           | <code>statistics</code> |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** When the log buffer is full, the subsequent logs are to be dropped, and an entry with all attributes "-" is displayed in the log buffer. The administrator shall increase the capacity of the log buffer or improve the rate of generating the syslog.

The generated syslog in the log buffer carries with the timestamp, for example:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED:
```

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)
```

**Configuration Examples** The following example displays the NFPP log configuration.

```

Hostname#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
VLAN 1-3, 5
interface Gi 0/1
interface Gi 0/2

```

The following example displays the log number in the buffer.

```

Hostname#show nfpp log buffer statistics
There are 6 logs in buffer.

```

The following example displays the NFPP log buffer:



```

Hostname#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address      Reason      Timestamp
-----
ARP      1      Gi0/1    1.1.1.1   -      DoS          2009-05-30
16:23:10
ARP      1      Gi0/1    1.1.1.1   -      ISOLATED     2009-05-30
16:23:10
ARP      1      Gi0/1    1.1.1.2   -      DoS          2009-05-30
16:23:15
ARP      1      Gi0/1    1.1.1.2   -      ISOLATE_FAILED 2009-05-30
16:23:15
ARP      1      Gi0/1    -          -      0000.0000.0001 SCAN          2009-05-30
16:30:10
ARP      -      Gi0/2    -          -      PORT_ATTACKED 2009-05-30
16:30:10
    
```

| Field    | Description                                                              |
|----------|--------------------------------------------------------------------------|
| Protocol | ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT                       |
| Reason   | 1. DoS<br>2. ISOLATED<br>3. ISOLATE_FAILE<br>4. SCAN<br>5. PORT_ATTACKED |

**Related Commands**

| Command               | Description                 |
|-----------------------|-----------------------------|
| <b>clear nfpp log</b> | Clears the NFPP log buffer. |

**Platform** N/A  
**Description**

### 1.90 show nfpp nd-guard summary

Use this command to display the configuration.

**show nfpp nd-guard summary**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the configuration.

**Examples**

```

Hostname# show nfpp nd-guard summary
(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold
Global      Enable  20/5/10    40/10/20
Gi 0/1      Enable  15/15/15   30/30/30
Gi 0/2      Disable -/5/30     -/10/50
    
```

| Field             | Description                                                             |
|-------------------|-------------------------------------------------------------------------|
| Interface(Global) | Global configuration mode.                                              |
| Status            | Enables/Disables the anti-attack function.                              |
| Rate-limit        | In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT. |
| Attack-threshold  | In the same format as the rate-limit.                                   |
| -                 | No configuration.                                                       |

**Related Commands**

| Command                          | Description                                           |
|----------------------------------|-------------------------------------------------------|
| <b>nd-guard attack-threshold</b> | Sets the global attack threshold.                     |
| <b>nd-guard enable</b>           | Enables the ND anti-attack function.                  |
| <b>nd-guard rate-limit</b>       | Sets the global rate-limit threshold.                 |
| <b>nfpp nd-guard enable</b>      | Enables the ND anti-attack function on the interface. |
| <b>nfpp nd-guard policy</b>      | Sets the rate-limit threshold and attack threshold.   |

**Platform** N/A

**Description**

### 1.91 show nfpp nd-guard trusted-host

Use this command to display the trusted host.

**show nfpp nd-guard trusted-host**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command** Privileged EXEC mode  
**Mode**

**Usage Guide** N/A

**Configuration** The following example displays the trusted host.

**Examples**

```

Hostname# show nfpp nd-guard trusted-host
mac
-----
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

# 1 Password Policies Commands

## 1.1 password policy life-cycle

Use this command to set the password lifecycle. Use the **no** form of this command to restore the default setting.

**password policy life-cycle days**


**no password policy life-cycle**

| Parameter Description | Parameter   | Description                                                                    |
|-----------------------|-------------|--------------------------------------------------------------------------------|
|                       | <i>days</i> | Sets the password lifecycle, in the range from 1 to 65535 in the unit of days. |

**Defaults** No password lifecycle is set by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration Examples** The following example sets the password lifecycle to 90 days.

```
Hostname(config)# password policy life-cycle 90
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 password policy min-size

Use this command to set the minimum length of the password. Use the **no** form of this command to restore the default setting.

**password policy min-size length**


**no password policy min-size**

| Parameter Description | Parameter     | Description                                                         |
|-----------------------|---------------|---------------------------------------------------------------------|
|                       | <i>length</i> | Sets the minimum length of the password, in the range from 1 to 31. |

**Defaults** No minimum length of the password is set by default.

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to set the minimum length of the password,

-  This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration** The following example sets the minimum length of the password to 8.

**Examples**

```
hostname(config)# password policy min-size 8
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

### 1.3 password policy no-repeat-times

Use this command to ban the use of passwords used in the past several times. Use the no form of this command to restore the default setting.

**password policy no-repeat-times times**


**no password policy no-repeat-times**

| Parameter Description | Parameter    | Description                                                                      |
|-----------------------|--------------|----------------------------------------------------------------------------------|
|                       | <i>times</i> | The past several times when passwords are configured, in the range from 1 to 31. |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails. This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration** The following example bans the use of passwords used in the past five times.

**Examples**

```
Hostname(config)# password policy no-repeat-times 5
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.4 password policy strong

Use this command to enable strong password check.

**password policy strong**  
**no password policy strong**

**Parameter Description**


| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

 This function is valid for the global password (the **enable password** and the **enable secret** commands) and the local user password (the **username name password password** command) while not valid for the password in line mode.

**Configuration** The following example configures the strong password check.

**Examples**

```
Hostname(config)# password policy strong
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.5 service password-encryption

Use this command to encrypt a password. Use the **no** form of this command to restore default setting.  
**service password-encryption**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the **service password-encryption** and **show running** or **write** command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.

**Configuration** The following example encrypts the password:

**Examples**

```
Hostname(config)# service password-encryption
```

| Related Commands | Command                | Description                             |
|------------------|------------------------|-----------------------------------------|
|                  | <b>enable password</b> | Sets passwords of different privileges. |

**Platform Description** N/A

## 1.6 show password policy

Use this command to display the password security policy set by the user.

**show password policy**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** This command is used to display the password security policy set by the user.

**Configuration Examples** The following example displays the password security policy set by the user.

```

Hostname#show password policy
Global password policy configurations:
  Password encryption:           Enabled
  Password strong-check:        Enabled
  Password min-size:             Enabled (6 characters)
  Password life-cycle:          Enabled (90 days)
  Password no-repeat-times:     Enabled (max history record: 5)
    
```

| Field                    | Description                                        |
|--------------------------|----------------------------------------------------|
| Password encryption      | Whether to encrypt the password.                   |
| Password strong-check    | Whether to enable password strong-check.           |
| Password min-size        | Whether to set the minimum length of the password. |
| Password life-cycle      | Whether to set the password lifecycle.             |
| Password no-repeat-times | Whether to ban recently-used passwords.            |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A



# 1 SSH Commands

## 1.1 crypto key generate

Use this command to generate a public key to the SSH server.

**crypto key generate** { *rsa* | *dsa* }




| Parameter   | Parameter  | Description           |
|-------------|------------|-----------------------|
| Description | <b>rsa</b> | Generates an RSA key. |
|             | <b>dsa</b> | Generates a DSA key.  |

**Defaults** By default, the SSH server does not generate a public key.

**Command** Global configuration mode

**Mode**

**Usage Guide** When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command **enable service ssh-server** at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.

-  Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.
-  RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.
-  A key can be deleted by using the **no crypto key generate** command. The **no crypto key zeroize** command is not available.

**Configuration** The following example generates an RSA key to the SSH server.

**Examples**

```

Hostname# configure terminal
Hostname(config)# crypto key generate rsa

```

| Related  | Command                                               | Description                                                    |
|----------|-------------------------------------------------------|----------------------------------------------------------------|
| Commands | <b>show ip ssh</b>                                    | Displays the current status of the SSH server.                 |
|          | <b>crypto key zeroize</b> { <i>rsa</i>   <i>dsa</i> } | Deletes DSA and RSA keys and disables the SSH server function. |

**Platform** N/A

**Description**

## 1.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

**crypto key zeroize** { *rsa* | *dsa* }

| Parameter   | Parameter  | Description          |
|-------------|------------|----------------------|
| Description | <b>rsa</b> | Deletes the RSA key. |
|             | <b>dsa</b> | Deletes the DSA key. |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the **no enable service ssh-server** command.

**Configuration** The following example deletes a RSA key to the SSH server.

**Examples**

```

Hostname# configure terminal
Hostname(config)# crypto key zeroize rsa

```

| Related Commands | Command                                                | Description                                    |
|------------------|--------------------------------------------------------|------------------------------------------------|
|                  | <b>show ip ssh</b>                                     | Displays the current status of the SSH server. |
|                  | <b>crypto key generate</b> { <i>rsa</i>   <i>dsa</i> } | Generates DSA and RSA keys.                    |

**Platform** N/A

**Description**

## 1.3 disconnect ssh

Use this command to disconnect the established SSH connection.

**disconnect ssh** [ *vty* ] *session-id*

| Parameter   | Parameter         | Description                                                     |
|-------------|-------------------|-----------------------------------------------------------------|
| Description | <b>vty</b>        | Established VTY connection                                      |
|             | <i>session-id</i> | ID of the established SSH connection, in the range from 0 to 35 |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.

**Configuration Examples** The following example disconnects the established SSH connection by specifying the SSH session ID.

```
Hostname# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Hostname# disconnect ssh vty 1
```

**Related Commands**

| Command                                  | Description                                                    |
|------------------------------------------|----------------------------------------------------------------|
| <b>show ssh</b>                          | Displays the information about the established SSH connection. |
| <b>clear line vty <i>line_number</i></b> | Disconnects the current VTY connection.                        |

**Platform** N/A

**Description**

## 1.1 disconnect ssh-session

Use this command to disconnect the suspended SSH client connection.

**disconnect ssh-session *session-id***

**Parameter Description**

| Parameter         | Description                                                   |
|-------------------|---------------------------------------------------------------|
| <i>session-id</i> | Specifies the ID of an SSH client session to be disconnected. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 1

**Usage Guide** You can enter the SSH client connection session ID to disconnect the specified SSH client connection.

**Configuration Examples** Enter the SSH client connection session ID to disconnect the specified SSH client connection.

```
Hostname# disconnect ssh-session 1
```

**Verification** Run the **show ssh-session** command to check whether the specified SSH client connection is terminated.

**Notifications** -

**Common** -

## Errors

## Platform

## Description

## 1.4 ip scp server enable

Use this command to enable the SCP server function on a network device.

Use the **no** form of this command to restore the default setting.

**ip scp server enable**

**no ip scp server enable**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.

**Configuration** The following example enables the SCP server function.

**Examples**

```
Hostname# configure terminal
Hostname(config)# ip scp server enable
```

| Related  | Command            | Description                                    |
|----------|--------------------|------------------------------------------------|
| Commands | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 1.2 ip ssh access-class

Use this command to configure an ACL on the SSH server.

**ip ssh access-class** { *access-list-number* | *access-list-name* }

Use the **no** form of this command to delete an ACL on the SSH server.

**no ip ssh access-class**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                               |                                                                                                                                                                                                         |                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b>            | <i>access-list-number</i>                                                                                                                                                                               | Specifies the ACL number. The IP standard ACL number ranges from 1 to 99 or 1300 to 1999, and the IP extended ACL ranges from 100 to 199 or 2000 to 2699. |
|                               | <i>access-list-name</i>                                                                                                                                                                                 | Specifies the ACL name.                                                                                                                                   |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                     |                                                                                                                                                           |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                                               |                                                                                                                                                           |
| <b>Defaults</b>               | 14                                                                                                                                                                                                      |                                                                                                                                                           |
| <b>Usage Guide</b>            | This command can be used to apply ACLs to all connections with the SSH server. In line mode, ACLs are valid only for specific lines. However, ACLs on the SSH server are valid for all SSH connections. |                                                                                                                                                           |
| <b>Configuration Examples</b> | The following example configures ACL testv4 for the SSH server.                                                                                                                                         |                                                                                                                                                           |
|                               | <pre> Hostname# configure terminal Hostname(config)# ip ssh access-class testv4 </pre>                                                                                                                  |                                                                                                                                                           |
| <b>Common Errors</b>          | -                                                                                                                                                                                                       |                                                                                                                                                           |
| <b>Notifications</b>          | -                                                                                                                                                                                                       |                                                                                                                                                           |
| <b>Common Errors</b>          | -                                                                                                                                                                                                       |                                                                                                                                                           |
| <b>Platform Description</b>   | -                                                                                                                                                                                                       |                                                                                                                                                           |

## 1.5 ip ssh authentication-retries

Use this command to set the authentication retry times of the SSH server.

Use the **no** form of this command to restore the default setting.

**ip ssh authentication-retries** *retry-times*

**no ip ssh authentication-retries**

| Parameter          | Parameter          | Description                                     |
|--------------------|--------------------|-------------------------------------------------|
| <b>Description</b> | <i>retry-times</i> | Authentication retry times, ranging from 0 to 5 |

**Defaults** The default is 3.

**Command** Global configuration mode

**Mode**

**Usage Guide** User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the **show ip ssh** command to display the configuration of the SSH server

**Configuration** The following example sets the authentication retry times to 2.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip ssh authentication-retries 2

```

| Related Commands | Command            | Description                                    |
|------------------|--------------------|------------------------------------------------|
|                  | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 1.6 ip ssh cipher-mode

Use this command to set the SSH server encryption mode.

Use the **no** form of this command to restore the default setting.

**ip ssh cipher-mode { cbc | ctr | others }**

**no ip ssh cipher-mode**

| Parameter Description | Parameter     | Description                                                                                                                                   |
|-----------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>cbc</b>    | Encryption mode: CBC (Cipher Block Chaining)<br>Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC |
|                       | <b>ctr</b>    | Encryption mode: CTR (Counter)<br>Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR                                                    |
|                       | <b>others</b> | Encryption mode: Others<br>Encryption algorithm: RC4                                                                                          |

**Defaults** All encryption modes are supported by default.

**Command** Global configuration mode

**Mode**

**Usage Guide** This command is used to set the SSH server encryption mode.

For Ruijie Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above.

With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and

enterprises demanding high security.

**Configuration** The following example enables CTR encryption mode.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip ssh cipher-mode ctr

```

**Platform** N/A

**Description**

## 1.7 ip ssh hmac-algorithm

Use this command to set the algorithm for message authentication.

Use the **no** form of this command to restore the default setting.

**ip ssh hmac-algorithm { md5 | md5-96 | sha1 | sha1-96 }**

**no ip ssh hmac-algorithm**

| Parameter          | Parameter      | Description       |
|--------------------|----------------|-------------------|
| <b>Description</b> | <b>md5</b>     | MD5 algorithm     |
|                    | <b>md5-96</b>  | MD5-96 algorithm  |
|                    | <b>sha1</b>    | SHA1 algorithm    |
|                    | <b>sha1-96</b> | SHA1-96 algorithm |

**Defaults** SSHv1: all the algorithms are not supported.

SSHv2: all the algorithms are supported.

**Command** Global configuration mode

**Mode**

**Usage Guide** Ruijie SSHv1 servers do not support algorithms for message authentication.

For Ruijie Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.

**Configuration** The following example sets the algorithm for message authentication to SHA1.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip ssh hmac-algorithm sha1

```

**Platform** N/A

**Description**

## 1.3 ip ssh key-exchange

Use this command to configure a DH key exchange algorithm supported by the SSH server.

**ip ssh key-exchange { dh\_group\_exchange\_sha1 | dh\_group1\_sha1 | dh\_group14\_sha1 }**

Use the **no** form of this command to restore the default DH key exchange algorithm supported by the SSH server.

**no ip ssh key-exchange**

| Parameter Description | Parameter                     | Description                                                                                                                                       |
|-----------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>dh_group_exchange_sha1</b> | Sets the DH key exchange algorithm to diffie-hellman-group-exchange-sha1. The default key length is <b>2048</b> bytes, which is not configurable. |
|                       | <b>dh_group1_sha1</b>         | Sets the DH key exchange algorithm to diffie-hellman-group1-sha1. The key length is 1024 bytes.                                                   |
|                       | <b>dh_group14_sha1</b>        | Sets the DH key exchange algorithm to diffie-hellman-group14-sha1. The key length is 2048 bytes.                                                  |

**Defaults** By default, the SSHv1 server does not support DH key exchange algorithms, and the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** This command is used to configure a DH key exchange algorithm supported by the SSH server. The SSHv1 server does not support any DH key exchange algorithm. The SSHv2 server supports the following DH key exchange algorithms: diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1. You can select DH key exchange algorithms supported by the SSH server as required.

**Configuration Examples** The following example sets the DH key exchange algorithm supported by the SSH server to diffie-hellman-group14-sha1.

```

Hostname# configure terminal
Hostname(config)# ip ssh key-exchange dh_group14_sha1

```

**Verification** -

**Notifications** -

**Common Errors** -

**Platform Description** -



## 1.8 ip ssh peer

Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name.

Use the **no** form of this command to restore the default setting.

**ip ssh peer** *username* **public-key** { *rsa* | *dsa* } *filename*

**no ip ssh peer** *username* **public-key** { *rsa* | *dsa* } *filename*

| Parameter   | Parameter       | Description                 |
|-------------|-----------------|-----------------------------|
| Description | <i>username</i> | User name                   |
|             | <i>filename</i> | Name of a public key file   |
|             | <b>rsa</b>      | The public key is a RSA key |
|             | <b>dsa</b>      | The public key is a DSA key |

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets RSA and DSA key files associated with user **test**.

```

Hostname# configure terminal
Hostname(config)# ip ssh peer test public-key rsa flash:rsa.pub
Hostname(config)# ip ssh peer test public-key dsa flash:dsa.pub

```

| Related  | Command            | Description                                    |
|----------|--------------------|------------------------------------------------|
| Commands | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 1.4 ip ssh port

Use this command to configure the listening port number of the SSH server.

**ip ssh port** *port*

Use the **no** form of this command to restore the default listening port number of the SSH server.

**no ip ssh port**

| Parameter   | Parameter   | Description                                                              |
|-------------|-------------|--------------------------------------------------------------------------|
| Description | <i>port</i> | Listening port of the SSH server. The value range is from 1025 to 65535. |

**Defaults** The default listening port number of the SSH server is 22.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example sets the listening port of the SSH server to **10000**.

```
Hostname# configure terminal
Hostname(config)# ip ssh port 10000
```

**Verification** Run the **show ip ssh** command to check the listening port number of the SSH server.

**Notifications** When the configured port is the same as the current value, the following notification will be displayed:

```
Hostname(config)# ip ssh port 22
% SSH tcp-port has been 22
```

If the configured port number is already in listening state, the system displays a message indicating that the port number is already in use, and another port number needs to be used. Otherwise, the device will continue to use the old port number.

```
Hostname(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port, otherwise the system will use the old tcp-port(22)!
```

When an error occurs after the configured listening port starts listening, the following notification will be displayed:

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

When a listening port is successfully configured, the following notification will be displayed:

```
Hostname(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

**Common Errors**

-

**Platform**

-

**Description**

## 1.9 ip ssh time-out

Use this command to set the authentication timeout for the SSH server.

Use the **no** form of this command to restore the default setting.

**ip ssh time-out** *time*

**no ip ssh time-out**

| Parameter   | Parameter   | Description                                                               |
|-------------|-------------|---------------------------------------------------------------------------|
| Description | <i>time</i> | Authentication timeout, in the range from 1 to 120 in the unit of seconds |

**Defaults** The default is 120 seconds.

**Command Mode** Global configuration mode

**Usage Guide** The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the **show ip ssh** command to display the configuration of the SSH server.

**Configuration** The following example sets the timeout value to 100 seconds.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip ssh time-out 100

```

| Related  | Command            | Description                                    |
|----------|--------------------|------------------------------------------------|
| Commands | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 1.10 ip ssh version

Use this command to set the version of the SSH server.

Use the **no** form of this command to restore the default setting.

**ip ssh version** { 1 / 2 }

**no ip ssh version**

| Parameter   | Parameter | Description                                  |
|-------------|-----------|----------------------------------------------|
| Description | <b>1</b>  | Supports the SSH1 client connection request. |
|             | <b>2</b>  | Supports the SSH2 client connection request. |

**Defaults** SSH1 and SSH2 are compatible by default.

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the **show ip ssh** command to display the current status of SSH server.

**Configuration** The following example sets the version of the SSH server.

**Examples**

```

Hostname# configure terminal
Hostname(config)# ip ssh version 2

```

| Related Commands | Command            | Description                                    |
|------------------|--------------------|------------------------------------------------|
|                  | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 1.5 ipv6 ssh access-class

Use this command to configure an IPv6 ACL on the SSH server.

**ipv6 ssh access-class** *accessv6-list-name*

Use the **no** form of this command to delete an IPv6 ACL on the SSH server.

**no ipv6 ssh access-class**

| Parameter Description | Parameter                 | Description                                          |
|-----------------------|---------------------------|------------------------------------------------------|
|                       | <i>accessv6-list-name</i> | Specifies the name of an IPv6 ACL on the SSH server. |

**Defaults** An IPv6 ACL is not configured on the SSH server.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** This command can be used to apply IPv6 ACLs to all connections with the SSH server. In line mode, IPv6 ACLs are valid only for specific lines. However, IPv6 ACLs on the SSH server are valid for all SSH connections.

**Configuration Examples** The following example configures IPv6 ACL **testv6** for the SSH server.

```

Hostname# configure terminal
Hostname(config)# ipv6 ssh access-class testv6

```

**Verification** -

- Notifications -
- Common -
- Errors -
- Platform -
- Description -

## 1.11 show crypto key mypubkey

Use this command to display the information about the public key part of the public key to the SSH server.

**show crypto key mypubkey { rsa | dsa }**

| Parameter   | Parameter | Description           |
|-------------|-----------|-----------------------|
| Description | rsa       | Displays the RSA key. |
|             | dsa       | Displays the DSA key. |

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.

**Configuration Examples** The following example displays the information about the public key part of the public key to the SSH server.

```

Hostname#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA1 private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
      AAAAAwEA AQAAAEAA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O
Q10kz+4/
      /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWlfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:

```

```
AAAAAwEA AQAAAEAA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi
BbzGZvn3
LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i80AkQ==
```

| Related  | Command                                        | Description                 |
|----------|------------------------------------------------|-----------------------------|
| Commands | <code>crypto key generate { rsa   dsa }</code> | Generates DSA and RSA keys. |

**Platform** N/A  
**Description**

## 1.12 show ip ssh

Use this command to display the information of the SSH server.

**show ip ssh**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** This command is used to display the information of the SSH server, including the version, status, port number, encryption mode, message authentication algorithm, authentication timeout, and authentication retry count.

Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.

**Configuration** The following example displays the information of the SSH server.

```
Examples
SSH and SCP disabled:
Hostname# show ip ssh
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
SSH Port:                22
SSH Cipher Mode:         cbc,ctr,others
SSH HMAC Algorithm:      md5-96,md5,sha1-96,sha1,sha2-256,sha2-512
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
Hostname(config)#show ip ssh
SSH Enable - version 1.99
```

```
SSH Port: 22
SSH Cipher Mode: cbc, ctr, others
SSH HMAC Algorithm: md5-96, md5, sha1-96, sha1, sha2-256, sha2-512
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

| Field                                         | Description                                                               |
|-----------------------------------------------|---------------------------------------------------------------------------|
| SSH Enable/Disable                            | Whether the SSH server function is enabled                                |
| version 1 2                                   | SSH version supported by the SSH server                                   |
| please generate rsa and dsa key to enable SSH | Whether the RSA/DSA public key is generate enable the SSH server function |
| SSH Port                                      | Listening port of the SSH server                                          |
| SSH Cipher Mode                               | Encryption mode of the SSH server                                         |
| SSH HMAC Algorithm                            | Message authentication algorithm of the server                            |
| Authentication timeout                        | User authentication timeout time                                          |
| Authentication retries                        | Maximum number of authentication atte allowed                             |
| SSH SCP Server enaled/disabled                | Whether the SSH SCP server function is enabl                              |

| Related Commands | Command                              | Description                                             |
|------------------|--------------------------------------|---------------------------------------------------------|
|                  | <b>ip ssh version {1   2}</b>        | Configures the version for the SSH server.              |
|                  | <b>ip ssh time-out time</b>          | Sets the authentication timeout for the SSH server.     |
|                  | <b>ip ssh authentication-retries</b> | Sets the authentication retry times for the SSH server. |

**Platform** N/A

**Description**

### 1.13 show ssh

Use this command to display the information about the established SSH connection.

**show ssh**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**Defaults** N/A

**Command Mode** All modes except the user EXEC mode

**Usage Guide** This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.

**Configuration** The following example displays the information about the established SSH connection:

```

Examples
Hostname# show ssh
Connection Version Encryption      Hmac      Compress  State
Username
      0      1.5 blowfish                      zlib      Session started test
      1      2.0 aes256-cbc    hmac-sha1  zlib      Session started test
    
```

Field Description

| Field      | Description                      |
|------------|----------------------------------|
| Connection | VTY number                       |
| Version    | SSH version                      |
| Encryption | Encryption algorithm             |
| Hmac       | Message authentication algorithm |
| Compress   | Compress algorithm               |
| State      | Connection state                 |
| Username   | Username                         |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**





# Reliability Commands

---

1. RLDP Commands

# 1 RLDP Commands

## 1.1 rldp detect-interval

Use this command to configure the interval for a port to send Rapid Link Detection Protocol (RLDP) packets.

Use the **no** or **default** form of this command to restore the default setting.

**rldp detect-interval** *interval*

**no rldp detect-interval**

**default rldp detect-interval**

| Parameter Description | Parameter       | Description                                                                            |
|-----------------------|-----------------|----------------------------------------------------------------------------------------|
|                       | <i>interval</i> | Interval for a port to send RLDP packets, in seconds. The value range is from 1 to 15. |

**Defaults** 3.

**Command Mode** Global configuration mode

**Default Level** 14

**Command Mode** Global configuration mode

**Usage Guide** The command takes effect for the probe packets and loop packets only. In an environment with Spanning Tree Protocol (STP) enabled, we recommend that (interval x maximum detection count) + 1 should be smaller than the topology convergence time of STP.

**Configuration Examples** The following example sets the detection interval to 5s.

```
Hostname(config)# rldp detect-interval 5
```

**Prompts** N/A

**Platform** N/A

**Description**

## 1.2 rldp detect-max

Use this command to configure the maximum detection count for unidirectional or bidirectional link detection on a port to determine the maximum detection time. If a neighbor port does not make a response within the maximum detection time, the link is diagnosed as faulty.

Use the **no** or **default** form of this command to restore the default setting.

**rldp detect-max** *num*

**no rldp detect-max**

**default rldp detect-max**

| Parameter Description | Parameter  | Description                                                                                   |
|-----------------------|------------|-----------------------------------------------------------------------------------------------|
|                       | <i>num</i> | Maximum detection count. The value range is from 2 to 10, and the default value is <b>2</b> . |

**Defaults** 2.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Maximum detection time = (detection interval x maximum detection count) + 1

**Configuration Examples** The following example sets the maximum detection count to **5**.

```
Hostname(config)# rldp detect-max 5
```

**Prompts** N/A

**Common Errors** N/A

**Platform** N/A

**Description**

## 1.3 rldp enable

Use this command to enable RLDP globally.

Use the **no** or **default** form of this command to restore the default setting.

**rldp enable**

**no rldp enable**

**default rldp enable**

| Parameter              | Parameter                                                                    | Description |
|------------------------|------------------------------------------------------------------------------|-------------|
| Description            | N/A                                                                          | N/A         |
| Defaults               | RLDP is disabled by default.                                                 |             |
| Command Mode           | Global configuration mode                                                    |             |
| Default Level          | 14                                                                           |             |
| Usage Guide            | RLDP detection can be enabled on a port only after RLDP is enabled globally. |             |
| Configuration Examples | The following example enables RLDP detection.                                |             |
|                        | <pre>Hostname(config)# rldp enable</pre>                                     |             |
| Prompts                | N/A                                                                          |             |
| Common Errors          | N/A                                                                          |             |
| Platform Description   | N/A                                                                          |             |

## 1.4 rldp error-recover interval

Use this command to configure the interval for recovering RLDP failed ports.

Use the **no** or **default** form of this command to restore the default setting.

**rldp error-recover interval** *interval*

**no rldp error-recover interval**

**default rldp error-recover interval**

| Parameter     | Parameter                             | Description                                                                                                                  |
|---------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Description   | <i>interval</i>                       | Interval for recovering failed ports, in seconds. The value range is from 30 to 86400. No interval is configured by default. |
| Defaults      | No interval is configured by default. |                                                                                                                              |
| Command Mode  | Global configuration mode             |                                                                                                                              |
| Default Level | 14                                    |                                                                                                                              |

**Usage Guide** This command is used to recover RLDP failed ports regularly. Recovering RLDP failed ports regularly is disabled by default. When an RLDP port is restored from the error state regularly, RLDP detection on the port is restarted. If the port failure in the environment is rectified, RLDP maintains the normal state and the environment is restored to the normal state. If the port failure in the environment is not rectified, RLDP detection continues.

**Configuration** The following example sets the detection interval to 600s.

**Examples** `Hostname(config)# rldp error-recover interval 600`

**Prompts** N/A

**Common** N/A

**Errors**

**Platform** N/A

**Description**

## 1.5 rldp neighbor-negotiation

Use this command to enable neighbor negotiation.

Use the **no** or **default** form of this command to restore the default setting.

**rldp neighbor-negotiation**

**no rldp neighbor-negotiation**

**default rldp neighbor-negotiation**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** Neighbor negotiation is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** If the negotiation function is enabled, unidirectional or bidirectional link detection starts on a port after the port finds a neighbor through negotiation. Negotiation is considered successful if the port receives a prob packet from the neighbor.

**Configuration** The following example enables neighbor negotiation during RLDP detection.

**Examples** `Hostname#config`  
`Hostname(config)#rldp neighbor-negotiation`

|                             |     |
|-----------------------------|-----|
| <b>Prompts</b>              | N/A |
| <b>Common Errors</b>        | N/A |
| <b>Platform Description</b> | N/A |

## 1.6 rldp port

Use this command to specify the detection type and failure handling method on a port.

Use the **no** or **default** form of this command to restore the default setting.

**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port }**

**no rldp port { unidirection-detect | bidirection-detect | loop-detect }**

**default rldp port { unidirection-detect | bidirection-detect | loop-detect }**

| Parameter Description | Parameter                  | Description                                                                           |
|-----------------------|----------------------------|---------------------------------------------------------------------------------------|
|                       | <b>unidirection-detect</b> | Enables unidirectional link detection.                                                |
|                       | <b>bidirection-detect</b>  | Enables bidirectional link detection.                                                 |
|                       | <b>loop-detect</b>         | Enables loop detection.                                                               |
|                       | <b>warning</b>             | Sends a warning upon a failure.                                                       |
|                       | <b>shutdown-svi</b>        | Shuts down the switch virtual interface (SVI) to which a port belongs upon a failure. |
|                       | <b>shutdown-port</b>       | Shuts down a port upon a failure.                                                     |

**Defaults** No RLDP detection is configured by default.

**Command Mode** Interface configuration mode

**Default Level** 14

**Usage Guide** The configuration takes effect on layer-2 switching ports, layer-3 routed ports, layer-2 aggregate port (AP) member ports, and layer-3 AP member ports, but not on layer-2 APs or layer-3 APs.

The port that detects a downlink loop failure is at random. For example, if RLDP downlink loop detection is configured on downlink ports A and B, the configured failure handling method is warning on downlink port A and shutdown-port on downlink port B, and a downlink loop exists between ports A and B, port A may detect a downlink loop failure before port B. After the failure handling method on port A takes effect, port A no longer sends packets or detects the downlink loop status. Port B does not receive probe packets from port A and cannot detect downlink loop failures. As a result, the

downlink loop failure still exists in the environment. To ensure that downlink loop failures in actual scenarios can be rectified, the loop failure handling method configured on downlink ports in the same loop must be the same and cannot be warning.

The monitor policy can be configured in unidirectional link detection mode for association with the Ethernet Ring Protection Switching (ERPS) protocol to ensure that ERPS can detect unidirectional link connection in time.

**Configuration** The following example configures the RLDP detection type and failure handling method.

**Examples**

```

Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port
    
```

**Prompts** N/A

**Common** N/A

**Errors**

**Platform** N/A

**Description**

## 1.7 rldp reset

Use this command to recover all RLDP failed ports and restart detection.

**rldp reset**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** This command is used to recover failed ports. The **errdisable recovery** command can also be used to recover failed ports. For details, see SWITCH-INTF-SCG.doc.

**Configuration** The following example recovers RLDP failed ports.

**Examples**

```

Hostname#rldp reset
    
```

**Prompts** N/A

**Common** N/A

**Errors**

**Platform**

**Description**

## 1.8 show rldp

Use this command to display RLDP global, port, and neighbor information.

**show rldp [ interface *interface-type interface-number* ]**

| Parameter   | Parameter                              | Description |
|-------------|----------------------------------------|-------------|
| Description | <i>interface-type interface-number</i> | RLDP port.  |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 2

**Usage Guide** You can specify a port name to display RLDP status information on the port.

**Configuration** The following example displays RLDP status information.

**Examples**

```

Hostname#show rldp
rldp state          : disable
rldp hello interval: 3
rldp max hello      : 2
rldp local bridge   : 00d0.f822.37da
-----
GigabitEthernet 0/1
port state          : normal
neighbor bridge    : 0000.0000.0000
neighbor port      :
unidirection detect information:
  action: shutdown-port
  state  : normal
bidirection detect information:
  action: shutdown-port
  state  : normal
loop detect information:
  action: shutdown-port
    
```



```
state : normal
```

The following example displays the configuration of all the monitoring points on GigabitEthernet 0/1.

```

Hostname#show rldp interface GigabitEthernet 0/1
port state      : normal
local bridge    : 00d0.f822.37da
neighbor bridge : 00d0.f823.37db
neighbor port   : GigabitEthernet 0/1
unidirection detect information:
    action: shutdown-port
    state : normal
bidirection detect information:
    action: shutdown-port
    state : normal
loop detect information:
    action: shutdown-port
    state : normal
    
```

| Field           | Description                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| port state      | Current status of a port. If the port is normal, <b>normal</b> is displayed. If the port is faulty, <b>error</b> is displayed.          |
| local bridge    | Media access control (MAC) address of the local system. It is used to differentiate the local device from the neighbor device.          |
| neighbor bridge | MAC address of the neighbor system. It is used to differentiate the local device from the neighbor device.                              |
| action          | Failure handling method of a detection type.                                                                                            |
| state           | Status of a detection type. If no failure is detected, <b>normal</b> is displayed. If a failure is detected, <b>error</b> is displayed. |

**Prompts** N/A

**Platform** N/A

**Description**



## Network Management and Monitoring Commands

---

1. NTP Commands
2. SNTP Commands
3. FTP Server Commands
4. FTP Client Commands
5. TFTP Client Commands
6. SNMP Commands
7. RMON Commands
8. CWMP Commands

# 1 NTP Commands

## 1.1 no ntp

Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.

**no ntp**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** NTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** By default, NTP is disabled. However, once the NTP server or the NTP master clock, the NTP service will be enabled.

**Configuration Examples** The following example disables NTP.

```
Hostname(config)#no ntp
```

| Related Commands | Command           | Description              |
|------------------|-------------------|--------------------------|
|                  | <b>ntp server</b> | Specifies an NTP server. |

**Platform** N/A

**Description**

## 1.2 ntp access-group

Use this command to configure an access group to control NTP access. Use the **no** form of this command to remove the peer access group.

**ntp access-group { peer | serve | serve-only | query-only } access-list-number | access-list-name**

**no ntp access-group { peer | serve | serve-only | query-only } access-list-number | access-list-name**


| Parameter Description | Parameter   | Description                                                                                                                           |
|-----------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>peer</b> | Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list. |

|                           |                                                                                                                                                                          |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>serve</b>              | Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers. |
| <b>serve-only</b>         | Allows the device to receive only time requests from the servers specified in the access list.                                                                           |
| <b>query-only</b>         | Allows the device to receive only NTP control queries from servers specified in the access list.                                                                         |
| <i>access-list-number</i> | Specifies the ACL number. The value ranges from 1 to 99 or 1300 to 1999.                                                                                                 |
| <i>access-list-name</i>   | Specifies the ACL name.                                                                                                                                                  |

**Defaults** No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism).  
 The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: **peer**, **serve**, **serve-only**, **query-only**.  
 If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.

 NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

**Configuration Examples** The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1.

```

Hostname(config)# access-list 1 permit 192.168.1.1
Hostname(config)# ntp access-group serve-only 1
    
```

| Related Commands | Command               | Description |
|------------------|-----------------------|-------------|
|                  | <b>ip access-list</b> |             |

**Platform** N/A  
**Description**

### 1.3 ntp authenticate

Use this command to enable NTP authentication. Use the **no** form of this command to disable NTP authentication.

**ntp authenticate**  
**no ntp authenticate**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** Disabled.

**Command mode** Global configuration mode.

**Usage Guide** If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally.  
 NTP authentication is implemented through the trusted key specified by the **ntp authentication-key** and **ntp trusted-key** commands.

**Configuration Examples** After an authentication key is configured and specified as the global trusted key, enable NTP authentication.

```

Hostname(config)#ntp authentication-key 6 md5 woooooop
Hostname(config)#ntp trusted-key 6
Hostname(config)#ntp authenticate
  
```

**Related  
Commands**

| Command                       | Description                         |
|-------------------------------|-------------------------------------|
| <b>ntp authentication-key</b> | Sets the global authentication key. |
| <b>ntp trusted-key</b>        | Configures the global trusted key.  |

**Platform** N/A  
**Description**

## 1.4 ntp authentication-key

Use this command to configure an NTP authentication key. Use the **no** form of this command to remove the NTP authentication key.

**ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]  
**no ntp authentication-key** *key-id*

**Parameter  
Description**

| Parameter         | Description                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <i>key-id</i>     | Key ID, ranging from 1 to 4294967295.                                                                                               |
| <i>key-string</i> | Key string, the maximum length of the key string is 31 bytes when the key is not encrypted, and 64 bytes when the key is encrypted. |

|                 |                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>enc-type</i> | Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|

**Defaults** NTP authentication key is not configured by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure an NTP authentication key and enables the **MD5** algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the **ntp trusted-key** command.

You can configure up to 1024 NTP authentication keys. However, each server can support only one key.

**Configuration** The following example configures an NTP authentication key.

**Examples**

```
Hostname(config)#ntp authentication-key 6 md5 woooooop
```

| Related Commands | Command                 | Description                    |
|------------------|-------------------------|--------------------------------|
|                  | <b>ntp authenticate</b> | Enables NTP authentication.    |
|                  | <b>ntp trusted-key</b>  | Configures an NTP trusted key. |
|                  | <b>ntp server</b>       | Specifies an NTP server.       |

**Platform** N/A

**Description**

## 1.5 ntp interval

Run the **ntp interval** command to configure the interval for clock synchronization between the NTP client and NTP server.

Run the **no** form of this command to remove this configuration.

**ntp interval** *seconds*

**no ntp interval**

| Parameter Description | Parameter      | Description                                                                                                      |
|-----------------------|----------------|------------------------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Interval for clock synchronization, in seconds. The value range is from 10 to 2592000. The default value is 64s. |

**Defaults** The default value is 64.

**Command mode** Global configuration mode

**Default Level** 14

**Usage Guide** The interval configured by this command does not take effect immediately. If you need this configuration to take effect immediately, enable NTP before configuring the interval.  
If the NTP client has not successfully synchronized the time, it quickly synchronizes the time at an interval of 5s. After the successful synchronization, the NTP server synchronizes the time at the configured interval.

**Configuration** Set the interval for clock synchronization between the NTP client and NTP server.

**Examples**

```
Hostname(config)# ntp interval 3600
```

**Verification** Run the **show run** command to check NTP parameters.

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.6 ntp master

Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the **no** form of this command to remove the device as an authoritative NTP server.

**ntp master** [ *stratum* ]

**no ntp master**



**Parameter  
Description**

| Parameter      | Description                                                 |
|----------------|-------------------------------------------------------------|
| <i>stratum</i> | Stratum level. The range is from 1 to 15. The default is 8. |

**Defaults** N/A

**Command  
mode** Global configuration mode.

**Usage Guide** In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.

-  Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.
-  Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock source.

**Configuration Examples** The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12:

```
Hostname(config)# ntp master 12
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.7 ntp server

Use this command to specify a NTP server for the NTP client. Use the **no** form of this command to delete the specified NTP server.

```
ntp server { ip-addr | domain | ip domain | ipv6 domain } [ version version ] [ source interface ]  

[ key keyid ] [ prefer ]  

no ntp server { ip-addr | domain | ip domain | ipv6 domain }
```

**Parameter Description**


| Parameter        | Description                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <i>ip-addr</i>   | Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.                                                   |
| <i>domain</i>    | Sets the domain name of the NTP server, supporting IPv4 and IPv6.                                                                   |
| <i>version</i>   | Specifies the NTP version. The value range is from 1 to 3. The default is NTPv3.                                                    |
| <i>interface</i> | Specifies the source interface from which the NTP message is sent (L3 interface).                                                   |
| <i>keyid</i>     | Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295. |
| <b>prefer</b>    | Specifies the given NTP server as the preferred one.                                                                                |

**Defaults** In the MACC or FAT mode, the default NAT server is ntp.jst.mfeed.ad.jp or ntp.nict.jp.



**Command mode** Global configuration mode.

**Usage Guide** At present, device only supports clients other than servers. Up to 20 servers can be synchronized. To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server. In the same condition (for instance, precision), the prefer clock is used for synchronization.

 The source interface of NTP packets must be configured with the IP address and can be communicated with the peer.

**Configuration** The following example configures an NTP server.

**Examples** For IPv4: `Hostname(config)# ntp server 192.168.210.222`  
 For IPv6: `Hostname(config)# ntp server 10::2`

**Related Commands**

| Command             | Description   |
|---------------------|---------------|
| <code>no ntp</code> | Disables NTP. |

**Platform Description** N/A

## 1.8 ntp service disable

Use this command to disable the time synchronization service provided by NTP. Use the **no** form of this command to enable the time synchronization service provided by NTP.

**ntp service disable**  
**no ntp service disable**

**Parameter Description**


| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** NTP provides the time synchronization service by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** NTP works in client/server mode. After the NTP device synchronizes time from an external reliable clock source, it serves as the time server to provide the time synchronization service. If the device just needs to be served as an NTP client, configure this command to disable the time synchronization service.

 This command and the **ntp master** command are mutually exclusive. When **ntp master** is enabled, the time synchronization service cannot be disabled on the NTP server. If this command is configured, the **ntp master** command cannot be configured.

**Configuration** The following example disables the NTP time synchronization service.

**Example**

```
Hostname(config)# ntp service disable
```

**Verification** Run the **show run | in ntp** command to display the NTP configuration.

**Platform Description** Supported only by some products.

## 1.9 ntp trusted-key

Use this command to set a global trusted key. Use the **no** form of this command to remove the global trusted key.

**ntp trusted-key** *key-id*

**no ntp trusted-key** *key-id*

| Parameter Description | Parameter     | Description                                          |
|-----------------------|---------------|------------------------------------------------------|
|                       | <i>key-id</i> | Global trusted key ID, ranging from 1 to 4294967295. |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.

**Configuration** The following example configures an authentication key and sets it as a trusted key.

**Examples**

```
Hostname(config)#ntp authentication-key 6 md5 woooooop
Hostname(config)#ntp trusted-key 6
Hostname(config)#ntp server 192.168.210.222 key 6
```

| Related Commands | Command                       | Description                           |
|------------------|-------------------------------|---------------------------------------|
|                  | <b>ntp authenticate</b>       | Enables NTP authentication.           |
|                  | <b>ntp authentication-key</b> | Configures an NTP authentication key. |

|                   |                           |
|-------------------|---------------------------|
| <b>ntp server</b> | Configures an NTP server. |
|-------------------|---------------------------|

**Platform** N/A  
**Description**

### 1.10 ntp update-calendar

Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the **no** form of this command to remove this function.

**ntp update-calendar**  
**no ntp update-calendar**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |

**Defaults** By default, update the calendar periodically is not configured.

**Command mode** Global configuration mode.

**Usage Guide** By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

**Configuration** The following example configures the NTP update calendar periodically.

**Examples**

```
Hostname(config)# ntp update-calendar
```

| <b>Related Commands</b> | Command | Description |
|-------------------------|---------|-------------|
|                         | N/A     | N/A         |

**Platform** N/A  
**Description**

### 1.11 show ntp server

Use this command to display the NTP server configuration.

**show ntp server**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              |           |             |

|     |     |
|-----|-----|
| N/A | N/A |
|-----|-----|

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** N/A

**Configuration** The following example displays the NTP server.

**Examples**

```

Hostname# show ntp server
ntp-server          source      keyid      prefer  version
-----
-----
10::2              None      None      FALSE   3
192.168.210.222   None      None      FALSE   3
    
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.12 show ntp status

Use this command to display the NTP configuration.

**show ntp status**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode

**Usage Guide** Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.

**Configuration** The following example displays the NTP configuration.

**Examples**

```

Hostname# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
    
```

```
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is
2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC )
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description** N/A

# 1 SNTP Commands

## 1.1 sntp enable

Use this command to enable the SNTP function. Use the **no** form of this command to restore the default value.

**sntp enable**

**no sntp enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** SNTP is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example enables SNTP.

```
Hostname(config)# sntp enable
```

| Related Commands | Command          | Description                      |
|------------------|------------------|----------------------------------|
|                  | <b>show sntp</b> | Displays the SNTP configuration. |

**Platform Description** N/A

## 1.2 sntp interval

Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the **no** form of this command to restore the default synchronization interval.

**sntp interval seconds**

**no sntp interval**

| Parameter Description | Parameter      | Description                                                                       |
|-----------------------|----------------|-----------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Synchronization interval. The unit is second, and the range is from 60 to 65,535. |

**Defaults** The default synchronization interval is 1,800 seconds.

**Command mode** Global configuration mode.

**Usage Guide** To make the synchronization interval configuration effective, run the **sntp enable** command.

**Configuration Examples** The following example configures the synchronization interval to 3,600 seconds.

```
Hostname(config)# sntp interval 3600
```

**Related Commands**

| Command            | Description                      |
|--------------------|----------------------------------|
| <b>sntp enable</b> | Enables SNTP.                    |
| <b>show sntp</b>   | Displays the SNTP configuration. |

**Platform Description** N/A

### 1.3 sntp server

Use this command to specify an SNTP server. Use the **no** form of this command to remove the SNTP server.

**sntp server** { *ip-address* | *domain* } [ **source** *source-ip-address* ]  
**no sntp server**

**Parameter Description**

| Parameter                | Description                              |
|--------------------------|------------------------------------------|
| <i>ip-address</i>        | IP address of the SNTP server.           |
| <i>domain</i>            | The domain name of the SNTP server.      |
| <i>source-ip-address</i> | Specifies the source IP address of SNTP. |

**Defaults** No SNTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.

**Configuration Examples** The following example specifies an SNTP server in Internet.

**Examples**

```
Hostname(config)# sntp server 192.168.4.12
```

**Related Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                    |                                  |
|--------------------|----------------------------------|
| <b>show sntp</b>   | Displays the SNTP configuration. |
| <b>sntp enable</b> | Enables SNTP.                    |

**Platform** N/A

**Description**

## 1.4 show sntp

Use this command to display the SNTP configuration.

**show sntp**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

**Command mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the SNTP configuration.

**Examples**

```

Hostname# show sntp
SNTP state          : Enable
SNTP server         : 192.168.4.12
SNTP sync interval  : 60
Time zone           : +8
    
```

| Field         | Description                   |
|---------------|-------------------------------|
| state         | SNTP status                   |
| server        | Time synchronization server   |
| sync interval | Time synchronization interval |
| Time zone     | Current time zone             |

**Related Commands**

| Command            | Description   |
|--------------------|---------------|
| <b>sntp enable</b> | Enables SNTP. |

**Platform** N/A

**Description**



# 1 FTP Server Commands

## 1.1 ftp-server enable

Use this command to enable the FTP server.

**ftp-server enable**

Use the **default** form of this command to restore the default setting.

**default ftp-server enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** This function is disabled by default.

**Command Mode** Global configuration mode

**Usage Guide** When the FTP server is enabled, you can connect to the FTP server through the FTP client and perform operations such as file upload or download.  
 The FTP client can access files on the FTP server only after this command and **ftp-server topdir** are configured.

**Configuration Examples** The following example enables the FTP server, and allows the client to access only the **syslog** sub-directory.

```
Hostname(config)# ftp-server topdir /syslog
Hostname(config)# ftp-server enable
```

The following example disables the FTP server.

```
Hostname(config)# no ftp-server enable
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 ftp-server login timeout

Use this command to set the timeout interval for login to the FTP server.

**ftp-server login timeout** *time*

Use the **no** or **default** form of this command to restore the default setting.

**no ftp-server login timeout**

| Parameter Description | Parameter   | Description                                                     |
|-----------------------|-------------|-----------------------------------------------------------------|
|                       | <i>time</i> | FTP login timeout, in minutes. The value range is from 1 to 30. |

**Defaults** The default is 2 minutes.

**Command Mode** Global configuration mode

**Usage Guide** The timeout interval refers to the maximum time when your account is allowed online after you login to the server. If you don't perform authentication again before the timeout interval expires, you will be forced offline.

**Configuration Examples** The following example sets the timeout interval for login to the FTP server to 5 minutes.

```
Hostname(config)# ftp-server login timeout 5
```

The following example restores the default setting.

```
Hostname(config)# no ftp-server login timeout
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.3 ftp-server login times

Use this command to set the number of login attempts. Use the **no** or **default** form of this command to restore the default setting.

**ftp-server login times** *times*

**no ftp-server login times**

**default ftp-server login times**

|                               |                                                                                                                                                                                 |                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                                                                                                                                | <b>Description</b>                                            |
|                               | <i>times</i>                                                                                                                                                                    | Sets the number of login attempts, in the range from 1 to 10. |
| <b>Defaults</b>               | The default is 3.                                                                                                                                                               |                                                               |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                       |                                                               |
| <b>Usage Guide</b>            | The number of login attempts refers to the maximum count you are allowed to perform authentication. If the number of your login attempts exceeds 3, you will be forced offline. |                                                               |
| <b>Configuration Examples</b> | The following example sets the number of login attempts to 5.                                                                                                                   |                                                               |
|                               | <pre>Hostname(config)# ftp-server login times 5</pre>                                                                                                                           |                                                               |
|                               | The following example restores the default setting.                                                                                                                             |                                                               |
|                               | <pre>Hostname(config)# no ftp-server login times</pre>                                                                                                                          |                                                               |
| <b>Related Commands</b>       | <b>Command</b>                                                                                                                                                                  | <b>Description</b>                                            |
|                               | N/A                                                                                                                                                                             | N/A                                                           |
| <b>Platform Description</b>   | N/A                                                                                                                                                                             |                                                               |

## 1.4 ftp-server timeout

Use this command to set the FTP session idle timeout.

**ftp-server timeout** *time*

Use the **no** form of this command to remove this configuration.

**no ftp-server timeout**

Use the **default** form of this command to restore the default configuration.

**default ftp-server timeout**

|                              |                            |                                                                                    |
|------------------------------|----------------------------|------------------------------------------------------------------------------------|
| <b>Parameter Description</b> | <b>Parameter</b>           | <b>Description</b>                                                                 |
|                              | <i>time</i>                | Sets the session idle timeout, in the range from 1 to 3600 in the unit of minutes. |
| <b>Defaults</b>              | The default is 10 minutes. |                                                                                    |

**Command** Global configuration mode.  
**Mode**

**Usage Guide** This command is used to configure the FTP session idle timeout. If no operation is performed on the current session within the specified time (that is, the session is idle), the FTP server considers that the connection has failed and therefore releases the connection with the user.

The session idle timeout refers to the time from the completion of the last FTP operation to the start of the next FTP operation in an FTP session. After the server responds to an FTP client command (for example, after a file is completely transferred), the server starts to count the idle time again, and stops counting when the next FTP client command arrives. Therefore, the configuration of the idle timeout does not affect time-consuming file transfer operations.

**Configuration** The following example sets the idle timeout to 5 minutes.

**Examples**

```
Hostname(config)# ftp-server timeout 5
```

The following example restores the default FTP login timeout to 10 minutes.

```
Hostname(config)# no ftp-server timeout
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.5 ftp-server topdir

Use this command to set the directory range for the FTP client to access to the FTP server files. Use the **no** or **default** form of this command to restore the default setting.

**ftp-server topdir** *directory*

**no ftp-server topdir**

**default ftp-server topdir**

**Parameter  
Description**

| Parameter        | Description             |
|------------------|-------------------------|
| <i>directory</i> | Sets the top-directory. |

**Defaults** No top-directory is configured by default.

**Command** Global configuration mode.  
**Mode**

**Usage Guide** The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified. Without this command configured, FTP client fails to access to any file or directory on the FTP server.

**Configuration Examples** The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory.

```

Hostname(config)# ftp-server topdir /syslog
Hostname(config)# ftp-server enable
    
```

The following example restores the default setting.

```

Hostname(config)# no ftp-server topdir
    
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.6 ftp-server username password

Use this command to set the login username and password for the FTP server.

**ftp-server username** *username* [ **privilege level** ] **password** [ *type* ] *password*

Use the **no** form of this command to remove this configuration.

**no ftp-server username** *username*

Use the **no** form of this command to restore the default configuration.

**default ftp-server username** *username*

**Parameter Description**

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>username</i>        | Username used for login. The value is a case-sensitive string of 1 to 64 characters, and no space is allowed in the middle of the string. The username may contain English letters, half-width numbers, and half-width symbols.                                                                                                                       |
| <b>privilege level</b> | Specifies the level of the login user, which is used to control the read/write permissions of the user. The value range is from 0 to 15, and the default value is <b>1</b> . The levels are consistent with those defined by AAA. The range from 0 to 5 indicates read only, the range from 6 to 10 indicates write only, and the range from 11 to 15 |

|                 |                                                                                                                                                                                                                                                                                                                                               |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | indicates read and write. Whether this parameter is supported depends on the actual product version.                                                                                                                                                                                                                                          |
| <i>type</i>     | 0 indicates not encrypted, and 7 indicates encrypted.                                                                                                                                                                                                                                                                                         |
| <i>password</i> | Password used for login. The password must contain letters or numbers. Spaces can appear before or after the password, but will be ignored. Spaces in the middle of the password are regarded as part of the password. A plain-text password is a string of 1 to 25 characters, and a cipher-text password is a string of 4 to 52 characters. |

**Defaults** No username or password is set by default.

**Command Mode** Global configuration mode

**Usage Guide** You must configure a username and password for login to the FTP server to authenticate the client. The password and the user must be in one-to-one correspondence. The FTP server does not support login of anonymous users. If the username configuration is cleared, the FTP client cannot pass the authentication of the FTP server. The FTP client must provide both the correct username and password to log in to the FTP server.

You can configure at most 10 users for an FTP server.

A user with the read-only permission can only download files from the FTP server. A user with the write-only permission can only upload files to the server. A user with both the read and write permissions can upload and download files to or from the FTP server.

**Configuration Examples** The following example sets the username to user:

```
Hostname(config)# ftp-server username user password pass
```

The following example restores the default setting:

```
Hostname(config)# no ftp-server username user
```

**Notifications** When a user tries to log in to the FTP server before a username is configured on the server, the following notification will be displayed:

```
%FTPSRV-4-USER: Haven't config username!
```

When the configured username is too long, the following notification will be displayed:

```
Hostname(config)# $$$
```

Username abcdefghijklmn, \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$ is NULL or too long, max length is 64.

When a user tries to log in to the FTP server before a password is configured on the server, the following notification will be displayed:

```
%FTPSRV-4-PASS: Haven't config password!
```

When the configured cipher-text password is too short, the following notification will be displayed:

```
Hostname(config)#ftp-server username user password 7 2
Invalid encrypted password, min length is 4, max length is 52.
```

When the configured plain-text password is too long, the following notification will be displayed:

```
Hostname(config)#ftp-server username user password abcdefghijklmnopqrstuvwxyz
% Password is too long, max length is 25
```

- Common**
  - The configured username contains invalid characters, or is too long.
- Errors**
  - A user tries to log in to the FTP server before a username is configured on the server.
  - A user tries to log in to the FTP server before a password is configured on the server.
  - The configured password is too short or too long.
  - The password contains invalid characters.

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.7 show ftp-server

Use this command to show the status information of the FTP server.

**show ftp-server**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

- Usage Guide** The FTP server status information includes:
- Enabled/Disabled server
  - The FTP server top directory
  - The FTP server user information, including username, password and connection number. If connection is set up, the IP address, port, transmission type, active/passive mode is shown

**Configuration Examples** The following example displays the related status information of the FTP server:

```
Hostname#show ftp-server
```

```

ftp-server information
=====
enable : Y
topdir : tmp:/
timeout: 10min
username:aaaa      password:(PLAIN)bbbb      connect num[2]
    [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21]
                        client IP:192.168.21.26[3927]
    [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21]
                        client IP:192.168.21.26[3929]
username:a1        password:(PLAIN)bbbb      connect num[0]
username:a2        password:(PLAIN)bbbb      connect num[0]
username:a3        password:(PLAIN)bbbb      connect num[0]
username:a4        password:(PLAIN)bbbb      connect num[0]
username:a5        password:(PLAIN)bbbb      connect num[0]
username:a6        password:(PLAIN)bbbb      connect num[0]
username:a7        password:(PLAIN)bbbb      connect num[0]
username:a8        password:(PLAIN)bbbb      connect num[0]
username:a9        password:(PLAIN)bbbb      connect num[0]
    
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description**

N/A



# 1 FTP Client Commands

## 1.1 copy flash

Use this command to upload the file from the server to the device through FTP Client.

**copy flash:** *[ local-directory/ ] local-file ftp://username:password@dest-address [ /remote-directory ] /remote-file*

| Parameter Description | Parameter               | Description                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>username</i>         | The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.                                                                                                                                                                                        |
|                       | <i>password</i>         | The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.                                                                                                                                                                                        |
|                       | <i>dest-address</i>     | IP address of the target FTP Server.                                                                                                                                                                                                                                                                                                |
|                       | <i>remote-directory</i> | File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.                                                                                                                                                   |
|                       | <i>remote-file</i>      | Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.                                                                                                                                                                                                                           |
|                       | <i>local-directory</i>  | Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters. |
|                       | <i>local-file</i>       | Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.                                                                                                                                                                                                                            |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file".

**Examples**

```
Hostname# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

**Verification** Run the **show ftp-client** command to view the FTP client configurations.

```
Hostname> enable
Hostname# show ftp-client
      ftp-client information
=====
type: ASCII
mode: PORT
```

Check whether the **remote-file** file is configured on the FTP server.

Run the **dir** command to check whether the **remote-file** file is configured in the **home** directory of the Flash.

**Notifications** If the upload succeeds, the following notification will be displayed:

```
success
```

If the upload fails, you can find the corresponding error message after running the **debug ftp-client** command.

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.2 copy ftp

Use this command to download the file from the server to the device through FTP Client.

**copy** ftp://username:password@dest-address [ /remote-directory ] / remote-file flash:[ local-directory/ ] local-file]

**Parameter Description**

| Parameter               | Description                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>username</i>         | The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.                                                                                                                                                                                        |
| <i>password</i>         | The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.                                                                                                                                                                                        |
| <i>dest-address</i>     | IP address of the target FTP Server.                                                                                                                                                                                                                                                                                                |
| <i>remote-directory</i> | File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.                                                                                                                                                   |
| <i>remote-file</i>      | Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.                                                                                                                                                                                                                           |
| <i>local-directory</i>  | Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters. |
| <i>local-file</i>       | Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.                                                                                                                                                                                                                            |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory "home" on the local device, and changes the name to "local-file".

```
Hostname# copy ftp://user:pass@192.168.23.69/root/remote-file
flash:home/local-file
```

The following example uploads a file named "local file" from the directory "home" on the local device to the directory "root" on FTP Server, and changes the name to "remote-file".

```
Hostname# copy flash:home/local-file
ftp://user:pass@192.168.23.69/root/remote-file
```

**Verification** Run the **dir** command to check whether the **remote-file** file is configured in the **home** directory of the Flash.

**Notifications** If the upload succeeds, the following notification will be displayed:

```
success
```

If the upload fails, you can find the corresponding error message after running the **debug ftp-client** command.

**Related Commands**

| Command          | Description                               |
|------------------|-------------------------------------------|
| <b>copy tftp</b> | Uses the TFTP protocol to transfer files. |

**Platform Description** N/A

### 1.3 ftp-client ascii

Use this command to use ASCII mode for FTP transfer.

Use the **no** form of this command to restore the default setting.

**ftp-client ascii**

**no ftp-clientascii**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** The default FTP transfer mode is binary.

**Command Mode** Global configuration mode

**Usage Guide** When the **default ftp-client** command is configured, all the configurations of the FTP client are restored to the default configurations. That is, the data connection mode is PASV, the FTP transmission mode is Binary, and the client is not bound to any source IP address.

**Configuration Examples** The following example configures ASCII FTP transfer.

```
Hostname(config)# ftp-client ascii
```

The following example configures binary FTP transfer.

```
Hostname(config)# no ftp-client ascii
```

**Verification** Run the **show ftp-client** command to view the FTP client configurations.

```
Hostname> enable
Hostname# show ftp-client
```

```
ftp-client information
=====
type: ASCII
mode: PORT
```

**Notifications** If the configuration succeeds, no notification will be displayed.

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

### 1.4 ftp-client port

Use this command to configure PORT mode used for FTP data connection. Use the **no** form of this command to restore the default setting.

**ftp-client port**  
**no ftp-client port**

Use the **default** form of this command to restore the default setting.

**default ftp-client**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The default is PASV mode for FTP data connection.

**Command Mode** Global configuration mode.

**Usage Guide** This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client.

The **default** command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.

**Configuration** The following example configures PORT mode used for FTP data connection

**Examples**

```
Hostname(config)# ftp-client port
```

The following example configures PASV mode for FTP data connection.

```
Hostname(config)# no ftp-client port
```

The following example restores the default setting of the FTP Client.

```
Hostname(config)# default ftp-client
```

**Verification** Run the **show ftp-client** command to view the FTP client configurations.

```
Hostname> enable
Hostname# show ftp-client
      ftp-client information
=====
type: ASCII
mode: PORT
```

**Notifications** If the configuration succeeds, no notification will be displayed.

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.5 ftp-client source

Use this command to bind FTP Client with the source IP address of client and use this IP address to communicate with server.

**ftp-client source** { *ip-address* | *ipv6-address* | *interface-type interface-number* }

Use the **no** form of this command to disable source IP address binding.

**no ftp-client source**

Use the **default** form of this command to restore the default setting.

**default ftp-client**

**Parameter  
Description**

| Parameter                              | Description                                            |
|----------------------------------------|--------------------------------------------------------|
| <i>ip-address</i>                      | Source IP address of the client.                       |
| <i>ipv6-address</i>                    | Source IPv6 address of the client.                     |
| <i>interface-type interface-number</i> | Type and number of the source interface of the client. |

**Defaults** By default, the IP address is not bound with the client locally. Instead, it is selected by the route.

**Command** Global configuration mode  
**Mode**

**Usage Guide** When the **default ftp-client** command is configured, all the configurations of the FTP client are restored to the default configurations. That is, the data connection mode is PASV, the FTP transmission mode is Binary, and the client is not bound to any source IP address.

**Configuration** The following example binds FTP Client with source IP address 192.168.23.236.

**Examples**

```
Hostname(config)# ftp-client source 192.168.23.236
```

The following example binds FTP Client with source IP address 2003:0:0:0::2.

```
Hostname(config)# ftp-client source 2003:0:0:0::2
```

The following example disables source IP address binding.

```
Hostname(config)# no ftp-client source
```

The following example restores the default setting of the FTP Client.

```
Hostname(config)# default ftp-client
```

**Verification** Run the **show running** command to view the FTP client configurations.

**Notifications** If the configuration succeeds, no notification will be displayed.

If the bound IP address is not a local address, the following notification will be displayed:

```
Bind failed: the specified source address is non-local ip
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description** N/A

# 1 TFTP Client Commands

## 1.1 copy flash

Use this command to use the Trivial File Transfer Protocol (TFTP) client to upload files from the local device to the TFTP server.

**copy flash:** [ *local-directory/* ] *local-file* **tftp://***dest-address* [ *remote-directory* ]/*remote-file*

| Parameter Description | Parameter               | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>dest-address</i>     | IP address of the TFTP server to be accessed.                                                                                                                                                                                                                                                                                               |
|                       | <i>remote-directory</i> | File path on the TFTP server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working directory of the TFTP server is used.                                                                                                                            |
|                       | <i>remote-file</i>      | Name of the file on the TFTP server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.                                                                                                                                                                                                                |
|                       | <i>local-directory</i>  | File path on the local device. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. |
|                       | <i>local-file</i>       | Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.                                                                                                                                                                                                               |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example uploads the **local-file** file in the **flash** directory on the device to the **root** directory of the TFTP server whose IP address is 192.168.23.69 and renames the file as **remote-file**.

```
Hostname# copy flash:local-file tftp://192.168.23.69/root/remote-file
```

**Verification** Check whether the **local-file** file exists in the **root** directory of the TFTP server. If the file exists, the upload is successful; otherwise, the upload fails.

**Prompts** If the upload fails, you can find the corresponding error message after running the **debug tftp** command. If



the upload is successful, "success" is displayed.

**Common Errors** N/A

**Platform Description** N/A

## 1.2 copy tftp

Use this command to use the TFTP client to download files from the TFTP server to the local device.

**copy tftp**://*dest-address*[ /*remote-directory* ]/*remote-file* **flash**:[ *local-directory*/ ]*local-file*

| Parameter Description | Parameter               | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>dest-address</i>     | IP address of the TFTP server to be accessed.                                                                                                                                                                                                                                                                                               |
|                       | <i>remote-directory</i> | File path on the TFTP server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. If this parameter is left empty, the current working directory of the TFTP server is used.                                                                                                                            |
|                       | <i>remote-file</i>      | Name of the file on the TFTP server. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.                                                                                                                                                                                                                |
|                       | <i>local-directory</i>  | File path on the local device. To specify a directory, ensure that the directory is already created. This command does not support automatic creation of a directory. If this parameter is left empty, the current directory of the device is used. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters. |
|                       | <i>local-file</i>       | Name of the file on the local device. It is a string of 1 to 255 characters, and cannot contain spaces or Chinese characters.                                                                                                                                                                                                               |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration Examples** The following example downloads the **remote-file** file from the **root** directory of the TFTP server whose IP address is 192.168.23.69 to the **flash** directory of the device and renames it as **local-file**.

```
Hostname# copy tftp://192.168.23.69/root/remote-file flash:local-file
```

**Verification** Run the **dir** command to check whether the **local-file** file exists on the local device. If the file exists, the

download is successful; otherwise, the download fails.

**Prompts** If the download fails, you can find the corresponding error message after running the **debug tftp** command. If the download is successful, "success" is displayed.

**Common** N/A

**Errors**

**Platform** N/A

**Description**

### 1.3 tftp-client port

Use this command to configure the port number used by the TFTP client to connect with the TFTP server.

Use the **no** form of this command to cancel the configuration.

Use the **default** form of this command to restore the default setting.

**tftp-client port** *port-number*

**no tftp-client port**

**default tftp-client port**

| Parameter Description | Parameter          | Description                                                                                |
|-----------------------|--------------------|--------------------------------------------------------------------------------------------|
|                       | <i>port-number</i> | Port number. The default port number is <b>69</b> . The value range is from 1025 to 65534. |

**Defaults** Port 69 is used to connect with the TFTP server by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** This command is used to configure the port number used by the TFTP client to connect with the TFTP server.

**Configuration Examples** The following example configures the port number used by the TFTP client to connect with the TFTP server.

```
Hostname(config)# tftp-client port 20005
```

The following example restores the TFTP client to the default setting.

```
Hostname(config)# default tftp-client port
Hostname(config)# no tftp-client port
```

**Verification** Run the **show running-config** command to display the port configuration of the TFTP client.

**Prompts** The configuration succeeds, and no notification is displayed.

**Common** N/A

**Errors**

**Platform** N/A

**Description**

## 1.4 tftp-client source

Use this command to configure the source IP address used by the TFTP client to communicate with the TFTP server.

Use the **no** form of this command to cancel the configuration.

Use the **default** form of this command to restore the default setting.

**tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }

**no tftp-client source**

**default tftp-client source**

**Parameter Description**

| Parameter                              | Description        |
|----------------------------------------|--------------------|
| <i>ip-address</i>                      | IPv4 address.      |
| <i>ipv6-address</i>                    | IPv6 address.      |
| <i>interface-type interface-number</i> | Interface address. |

**Defaults** By default, no source IP address is bound to the TFTP client, and an IP address is selected for the client based on the route.

**Command** Global configuration mode

**Mode**

**Default Level** 14

**Usage Guide** This command is used to configure the source IP address used by the TFTP client to communicate with the TFTP server.

**Configuration** The following example sets the source IP address of the TFTP client to 192.168.23.236.

```
Hostname(config)# tftp-client source ip 192.168.23.236
```

The following example sets the source IP address of the TFTP client to 2003:0:0:0::2.

```
Hostname(config)# tftp-client source ipv6 2003:0:0:0::2
```

The following example binds the IP address of tenGigabitEthernet 1/0/1 to the TFTP client.

```
Hostname(config)# tftp-client source tenGigabitEthernet 1/0/1
```

The following example cancels the source IP address bound to the TFTP client.

```
Hostname(config)# no tftp-client source
```

The following example restores the TFTP client to the default setting.

```
Hostname(config)# default tftp-client source
```

**Verification** Run the **show running-config** command to display the IPv4 address configuration of the TFTP client.  
Run the **show running-config** command to display the IPv6 address configuration of the TFTP client.

**Prompts** If 192.168.23.236 is not a local address, an error is displayed. If it is a local address, the configuration succeeds and no notification will be displayed.  
If 2003:0:0:0::2 is not a local address, the following notification will be displayed: Bind failed: the specified source address is non-local ip. If it is a local address, the configuration succeeds and no notification will be displayed.  
The configuration succeeds, and no notification will be displayed.

**Common Errors** N/A

**Platform Description** N/A

# 1 SNMP Commands

## 1.1 clear snmp locked-ip

Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.

**clear snmp locked-ip** [ **ipv4** *ipv4-address* | **ipv6** *ipv6-address* ]

| Parameter Description | Parameter                       | Description                      |
|-----------------------|---------------------------------|----------------------------------|
|                       | <b>ipv4</b> <i>ipv4-address</i> | Clears a specified IPv4 address. |
|                       | <b>ipv6</b> <i>ipv6-address</i> | Clears a specified IPv6 address. |

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address.

After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.

**Configuration Examples** The following example clears the whole source IP address table locked after continuous SNMP authentication failures.

```
Hostname#clear snmp locked-ip
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 1.2 no snmp-server

Use this command to disable the SNMP agent function.

**no snmp-server**

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table> | Parameter | Description | N/A | N/A |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|-----|-----|
| Parameter                     | Description                                                                                                                                           |           |             |     |     |
| N/A                           | N/A                                                                                                                                                   |           |             |     |     |
| <b>Defaults</b>               | SNMP agent is enabled by default.                                                                                                                     |           |             |     |     |
| <b>Command mode</b>           | Global configuration mode.                                                                                                                            |           |             |     |     |
| <b>Usage Guide</b>            | This command disables the SNMP agent services of all versions supported on the device.                                                                |           |             |     |     |
| <b>Configuration Examples</b> | The following example disables the SNMP agent.<br><pre>Hostname(config)# <b>no snmp-server</b></pre>                                                  |           |             |     |     |
| <b>Related Commands</b>       | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table>   | Command   | Description | N/A | N/A |
| Command                       | Description                                                                                                                                           |           |             |     |     |
| N/A                           | N/A                                                                                                                                                   |           |             |     |     |
| <b>Platform Description</b>   | N/A                                                                                                                                                   |           |             |     |     |

### 1.3 show snmp

Use this command to display the SNMP configuration.

**show snmp [ mib | user | view | group | host | locked-ip | process-mib-time ]**

| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>mib</b></td> <td>Displays the SNMP MIBs supported.</td> </tr> <tr> <td><b>user</b></td> <td>Displays the SNMP user information.</td> </tr> <tr> <td><b>view</b></td> <td>Displays the SNMP view information.</td> </tr> <tr> <td><b>group</b></td> <td>Displays the SNMP user group information.</td> </tr> <tr> <td><b>host</b></td> <td>Displays the explicit host configuration.</td> </tr> <tr> <td><b>locked-ip</b></td> <td>Displays the source IP addresses locked after continuous SNMP authentication failures.</td> </tr> <tr> <td><b>process-mib-time</b></td> <td>Displays the MIB node requiring the longest processing time.</td> </tr> </tbody> </table> | Parameter | Description | <b>mib</b> | Displays the SNMP MIBs supported. | <b>user</b> | Displays the SNMP user information. | <b>view</b> | Displays the SNMP view information. | <b>group</b> | Displays the SNMP user group information. | <b>host</b> | Displays the explicit host configuration. | <b>locked-ip</b> | Displays the source IP addresses locked after continuous SNMP authentication failures. | <b>process-mib-time</b> | Displays the MIB node requiring the longest processing time. |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|------------|-----------------------------------|-------------|-------------------------------------|-------------|-------------------------------------|--------------|-------------------------------------------|-------------|-------------------------------------------|------------------|----------------------------------------------------------------------------------------|-------------------------|--------------------------------------------------------------|
| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>mib</b>                   | Displays the SNMP MIBs supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>user</b>                  | Displays the SNMP user information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>view</b>                  | Displays the SNMP view information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>group</b>                 | Displays the SNMP user group information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>host</b>                  | Displays the explicit host configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>locked-ip</b>             | Displays the source IP addresses locked after continuous SNMP authentication failures.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>process-mib-time</b>      | Displays the MIB node requiring the longest processing time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>Defaults</b>              | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>Command mode</b>          | Privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |
| <b>Usage Guide</b>           | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |             |            |                                   |             |                                     |             |                                     |              |                                           |             |                                           |                  |                                                                                        |                         |                                                              |

**Configuration** The example below displays the SNMP configuration:

**Examples**

```

Hostname# show snmp
Chassis: 60FF60
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors (Maximum packet size 1472)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP global trap: disabled
SNMP logging: disabled
SNMP agent: enabled
    
```

| Field                                         | Description                                                                         |
|-----------------------------------------------|-------------------------------------------------------------------------------------|
| Chassis                                       | System serial number                                                                |
| SNMP packets input                            | Total number of input packets                                                       |
| Bad SNMP version errors                       | Total number of packets with version error                                          |
| Unknown community name                        | Total number of packets in which an unknown community name is used for access       |
| Illegal operation for community name supplied | Total number of packets in which the community name is used for override operations |
| Encoding errors                               | Total number of packets with encoding error                                         |
| Number of requested variables                 | Total number of read MIB objects                                                    |
| Number of altered variables                   | Total number of set MIB objects                                                     |
| Get-request PDUs                              | Total number of Get request packets                                                 |
| Get-next PDUs                                 | Total number of Get-next request packets                                            |
| Set-request PDUs                              | Total number of Set request packets                                                 |
| SNMP packets output                           | Total number of output packets                                                      |

|                                           |                                                                  |
|-------------------------------------------|------------------------------------------------------------------|
| Too big errors (Maximum packet size 1472) | Total number of excessively long packets (more than 1,472 bytes) |
| No such name errors                       | Total number of packets that contains the no such name error     |
| Bad values errors                         | Total number of packets that contains the bad values error       |
| General errors                            | Total number of packets that contains the general error          |
| Response PDU                              | Total number of packets that are normally returned               |
| Trap PDUs                                 | Total number of sent Trap packets                                |
| SNMP global trap                          | Global Trap enabling/disabling status                            |
| SNMP logging                              | Global SNMP log enabling/disabling status                        |
| SNMP agent                                | Global SNMP agent enabling/disabling status                      |

#### Related Commands

| Command                       | Description                                |
|-------------------------------|--------------------------------------------|
| <b>snmp-server chassis-id</b> | Specifies the SNMP system sequence number. |

**Platform** N/A  
**Description**

## 1.4 snmp trap link-status

Use this command to enable the interface to send link traps. Use the **no** form of this command to disable the interface to send link traps.

**snmp trap link-status**

**no snmp trap link-status**

#### Parameter Description

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.

**Command mode** Interface configuration mode

**Usage Guide** This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.

**Configuration Examples** The following example disables the interface to send link traps.

```
Hostname(config)# interface gigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Hostname(config)# interface gigabitEthernet 0/1
```



```
Hostname(config-if-GigabitEthernet 0/1)# snmp trap link-status
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A

## 1.5 snmp-server authentication attempt

Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure.

Use the **no** form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.

**snmp-server authentication attempt *times* exceed { lock | lock-time *minutes* | unlock }**

**no snmp-server authentication attempt *times* exceed { lock | lock-time *minutes* | unlock }**

**Parameter  
Description**

| Parameter                       | Description                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>times</i>                    | Indicates the maximum number of continuous SNMP authentication failures. The range is from 1 to 10. The default value is 3.                                    |
| <b>exceed</b>                   | Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded.                                        |
| <b>lock</b>                     | Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration.           |
| <b>lock-time <i>minutes</i></b> | Indicates that the source IP address is locked for a period of time. The <i>minutes</i> indicates the lock time, ranging from 1 to 65,535. The unit is minute. |
| <b>unlock</b>                   | Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed.                   |

**Defaults** SNMP attack detection is enabled by default.

**Command mode** Global configuration mode

**Usage Guide** The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy:

1. For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually.

2. For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually.
3. For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.

**Configuration Examples** The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds.

```
Hostname(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.6 snmp-server chassis-id

Use this command to specify the SNMP chassis ID. Use the **no** form of this command to restore the default chassis ID.

**snmp-server chassis-id** *text*

**no snmp-server chassis-id**

**Parameter Description**

| Parameter   | Description                              |
|-------------|------------------------------------------|
| <i>text</i> | SNMP chassis ID: numerals or characters. |

**Defaults** The default is 60FF60.

**Command mode** Global configuration mode.

**Usage Guide** The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the **show snmp** command.

**Configuration Examples** The following example specifies the SNMP chassis ID as 123456:

```
Hostname(config)# snmp-server chassis-id 123456
```

**Related Commands**

| Command          | Description                      |
|------------------|----------------------------------|
| <b>show snmp</b> | Displays the SNMP configuration. |

**Platform Description** N/A

## 1.7 snmp-server community

Use this command to specify the SNMP community access string. Use the **no** form of this command to remove the SNMP community access string.

```
snmp-server community { [ 0 | 7 ] string | secret [ 0 | 8 ] string } [ view view-name ] [ [ ro | rw ] [ host ipaddr ] ] [ ipv6 ipv6-aclname ] [ aclnum | aclname ]
```

```
no snmp-server community { [ 0 | 7 ] string | secret [ 0 | 8 ] string }
```

### Parameter Description

| Parameter           | Description                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------|
| 0                   | Indicates that the community string is in plaintext.                                                                    |
| 7                   | Indicates that the community string is in ciphertext.                                                                   |
| <i>string</i>       | Community string, which is the communication password between the NMS and the SNMP agent                                |
| <b>secret</b>       | Indicates that the community name needs to be encrypted. SHA256 is used by default.                                     |
| <b>0</b>            | <b>0</b> indicates that the input community string is a plaintext string and is encrypted with the default algorithm.   |
| <b>8</b>            | <b>8</b> indicates that the input community string is a ciphertext string and is encrypted with the SHA256 algorithm.   |
| <i>view-name</i>    | View name                                                                                                               |
| <b>ro</b>           | Indicates that the NMS can only read the variables of the MIB.                                                          |
| <b>rw</b>           | Indicates that the NMS can read and write the variables of the MIB.                                                     |
| <i>aclnum</i>       | Indicates the ACL number (1–199 or 1300–2699), which specifies the IPv4 addresses that are permitted to access the MIB. |
| <i>aclname</i>      | Access list name, which specifies the IPv4 addresses that are permitted to access the MIB.                              |
| <i>ipv6-aclname</i> | IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.                         |
| <i>ipaddr</i>       | Specifies the IP address of the NMS to access the MIB.                                                                  |

**Defaults** All communities are read only by default.

**Command mode** Global configuration mode.

**Usage Guide** This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB.  
To disable the SNMP agent function, use the **no snmp-server** command.

**Configuration Examples** The following example defines a SNMP community access string named public, which can be read-only.

```
Hostname (config) # snmp-server community public ro
```

| Related Commands | Command            | Description             |
|------------------|--------------------|-------------------------|
|                  | <b>access-list</b> | Defines an access list. |

**Platform** N/A

**Description**

## 1.8 snmp-server contact

Use this command to specify the system contact string. Use the **no** form of this command to remove the system contact string.

**snmp-server contact** *text*

**no snmp-server contact**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           | <i>text</i> |

**Defaults** No system contact string is set by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies the SNMP system contract `i-net800@i-net.com.cn`:

**Examples**

```
Hostname (config) # snmp-server contact i-net800@i-net.com.cn
```

| Related Commands      | Command                           | Description                      |
|-----------------------|-----------------------------------|----------------------------------|
|                       | <b>show snmp-server</b>           | Displays the SNMP configuration. |
| <b>no snmp-server</b> | Disables the SNMP agent function. |                                  |

**Platform** N/A

**Description**

## 1.9 snmp-server enable secret-dictionary-check

Use this command to enable the secret dictionary check for the **community** and **user** fields. Use the **no** form of this command to disable the secret dictionary check.

**snmp-server enable secret-dictionary-check**

**no snmp-server enable secret-dictionary-check**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** Secret dictionary check for the **community** and **user** fields is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **password policy** command.

**Configuration Examples** The following example enables the secret dictionary check for the **community** field.

```

Hostname(config)# password policy min-size 6
Hostname(config)# snmp-server enable secret-dictionary-check
Hostname(config)#snmp-server community abc12
% The community(abc12) is a weak community!

```

| Related Commands | Command                 | Description                                            |
|------------------|-------------------------|--------------------------------------------------------|
|                  | <b>snmp-server host</b> | Specifies the SNMP host to send the SNMP trap message. |

**Platform** N/A  
**Description**

## 1.10 snmp-server enable traps

Use this command to enable the SNMP agent to send the SNMP trap message to NMS. Use the **no** form of this command to disable the SNMP agent to send the SNMP trap message to NMS.

**snmp-server enable traps** [ *notification-type* ]

**no snmp-server enable traps**

| Parameter Description | Parameter                | Description                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>notification-type</i> | Specifies the type of trap messages.<br>authentication: Allow authentication notifications.<br>snmp: SNMP trap message<br>bridge: Bridge trap message.<br>entity: entity Trap message.<br>mac-notification: MAC trap message.<br>nfpp: NFPP Traps message.<br>web-auth: Web authentication trap message. |

- Defaults** Sending trap message to the NMS is disabled by default.
- Command mode** Global configuration mode.
- Usage Guide** This command must be used together with the **snmp-server host** command to send the trap message. Specifying no trap type indicates all trap messages are sent.

**Configuration** The following example enables the SNMP agent to send the SNMP trap message.

**Examples**

```
Hostname(config)# snmp-server enable traps snmp
Hostname(config)# snmp-server host 192.168.12.219 public snmp
```

**Related Commands**

| Command                 | Description                                            |
|-------------------------|--------------------------------------------------------|
| <b>snmp-server host</b> | Specifies the SNMP host to send the SNMP trap message. |

**Platform** N/A

**Description**

## 1.11 snmp-server flow-control

Use this command to configure the SNMP flow control. Use the **no** form of this command to restore the default setting.

**snmp-server flow-control pps** *count*

**no snmp-server flow-control pps**

**Parameter Description**

| Parameter    | Description                                                                            |
|--------------|----------------------------------------------------------------------------------------|
| <i>count</i> | Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535. |

**Defaults** The default count is 300.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the number of SNMP requests processed per second to 200.

**Examples**

```
Hostname(config)# snmp-server flow-control pps 200
```

**Related Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|     |     |
|-----|-----|
| N/A | N/A |
|-----|-----|

**Platform** N/A  
**Description**

## 1.12 snmp-server group

Use this command to configure a new SNMP group. Use the **no** form of this command to remove a specified SNMP group.

**snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [ **read** *readview* ] [ **write** *writeview* ] [ **access** { [ **ipv6** *ipv6\_aclname* ] *aclnum* | *aclname* } ]

**no snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }

**Parameter Description**

| Parameter                          | Description                                                                                                             |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>v1</b>   <b>v2c</b>   <b>v3</b> | Specifies the SNMP version                                                                                              |
| <b>auth</b>                        | Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.                                |
| <b>noauth</b>                      | Specifies no authentication a packet. This applies to SNMPv3 only.                                                      |
| <b>priv</b>                        | Specifies authentication of a packet with encryption. This applies to SNMPv3 only.                                      |
| <i>readview</i>                    | Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.            |
| <i>writeview</i>                   | Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent. |
| <i>aclnum</i>                      | Access list number, which specifies the IPv4 addresses that are permitted to access the MIB.                            |
| <i>aclname</i>                     | Name of the access list, which specifies the IPv4 addresses that are permitted to access the MIB.                       |
| <i>ipv6_aclname</i>                | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.                  |

**Defaults** No SNMP groups are configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures a new SNMP group.

**Examples**

```
Hostname(config)# snmp-server group mib2user v3 priv read mib2
```

| Related Commands | Command | Description            |
|------------------|---------|------------------------|
|                  |         | <b>show snmp group</b> |

**Platform** N/A  
**Description**

## 1.13 snmp-server heartbeat on

Use this command to enable the heartbeat trap function. Use the **no** form of this command to disable this function.

**snmp-server heartbeat on**

**no snmp-server heartbeat on**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           | N/A         |

**Defaults** The heartbeat trap function is enabled by default.

**Command mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example disables the heartbeat trap function.

```
Hostname(config)# no snmp-server heartbeat on
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  |         | N/A         |

**Platform** N/A  
**Description**

## 1.14 snmp-server heartbeat period

Use this command to configure the interval for sending heartbeat trap messages. Use the **no** form of this command to restore the default interval.

**snmp-server heartbeat period *seconds***

**no snmp-server heartbeat period**



|                               |                                                                                                  |                                                                                                   |
|-------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                                                 | <b>Description</b>                                                                                |
|                               | <i>seconds</i>                                                                                   | Indicates the interval for sending heartbeat trap messages (unit: second).<br>Range: 60 to 3,600. |
| <b>Defaults</b>               | The default interval for sending heartbeat trap message is 300 seconds by default.               |                                                                                                   |
| <b>Command mode</b>           | Global configuration mode                                                                        |                                                                                                   |
| <b>Usage Guide</b>            | N/A                                                                                              |                                                                                                   |
| <b>Configuration Examples</b> | The following example configures the interval for sending heartbeat trap messages to 60 seconds. |                                                                                                   |
|                               | <pre>Hostname(config)# snmp-server heartbeat period 60</pre>                                     |                                                                                                   |
| <b>Related Commands</b>       | <b>Command</b>                                                                                   | <b>Description</b>                                                                                |
|                               | N/A                                                                                              | N/A                                                                                               |
| <b>Platform Description</b>   | N/A                                                                                              |                                                                                                   |

## 1.15 snmp-server host

Use this command to specify the SNMP host (NMS) to send the trap message. Use the **no** form of this command to remove the specified SNMP host.

```
snmp-server host { host-addr | ipv6 ipv6-addr } [ traps | informs ] [ version { 1 | 2c | 3 [ auth | noauth | priv ] ] community-string [ udp-port port-num ] [ notification-type ]
no snmp-server host { host-addr | ipv6 ipv6-addr } [ traps | informs ] [ version { 1 | 2c | 3 { auth | noauth | priv } ] community-string [ udp-port port-num ]
```

|                              |                                           |                                                                     |
|------------------------------|-------------------------------------------|---------------------------------------------------------------------|
| <b>Parameter Description</b> | <b>Parameter</b>                          | <b>Description</b>                                                  |
|                              | <i>host-addr</i>                          | SNMP host address                                                   |
|                              | <i>ipv6-addr</i>                          | SNMP host address(ipv6)                                             |
|                              | <b>trap</b>   <b>informs</b>              | Enables the host to send the SNMP notification as traps or informs. |
|                              | <b>version</b>                            | SNMP version: V1, V2C or V3                                         |
|                              | <b>auth</b>   <b>noauth</b>   <b>priv</b> | Security level of SNMPv3 users                                      |
|                              | <i>community-string</i>                   | Community string or username (SNMPv3 version)                       |
|                              | <i>port-num</i>                           | Port of the SNMP host. The value range is from 0 to 65535.          |
|                              | <i>notification-type</i>                  | The type of the SNMP trap message, such as <b>snmp</b> .            |

|  |                                                                                                        |
|--|--------------------------------------------------------------------------------------------------------|
|  | If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included. |
|--|--------------------------------------------------------------------------------------------------------|

**Defaults** No SNMP host is specified by default.

**Command mode** Global configuration mode.

**Usage Guide** This command must be used together with the **snmp-server enable traps** command to send the SNMP trap messages to NMS.

**Configuration Examples** The following example specifies an SNMP host to receive the SNMP event trap:

```
Hostname(config)# snmp-server host 192.168.12.219 public snmp
```

| <b>Related Commands</b> | Command                         | Description                                           |
|-------------------------|---------------------------------|-------------------------------------------------------|
|                         | <b>snmp-server enable traps</b> | Enables the SNMP agent to send the SNMP trap message. |

**Platform** N/A

**Description**

## 1.16 snmp-server inform

Use this command to configure the resend times for inform requests and the inform request timeout. Use the **no** form of this command to restore the default settings.

**snmp-server inform { retries *retry-time* | timeout *time* }**

**no snmp-server inform**

| <b>Parameter Description</b> | Parameter         | Description                                                                     |
|------------------------------|-------------------|---------------------------------------------------------------------------------|
|                              | <i>retry-time</i> | Specifies the resend times for inform requests, ranging from 0 to 255.          |
|                              | <i>time</i>       | Specifies the inform request timeout, in seconds, ranging from 0 to 21,474,836. |

**Defaults** The default *retry-num* is 3, and the default **timeout time** is 15 seconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the resend times of inform requests to 5.

**Examples** `Hostname(config)# snmp-server inform retries 5`

The following example configures the inform request timeout to 20 seconds.

`Hostname(config)# snmp-server inform timeout 20`

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 1.17 snmp-server location

Use this command to set the system location string. Use the **no** form of this command to remove the system location string.

**snmp-server location** *text*

**no snmp-server location**

**Parameter Description**

| Parameter   | Description                                            |
|-------------|--------------------------------------------------------|
| <i>text</i> | String that describes the system location information. |

**Defaults** No system location string is set by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example sets the system location information:

**Examples** `Hostname(config)# snmp-server location start-technology-city 4F of A Buliding`

**Related Commands**

| Command                    | Description                          |
|----------------------------|--------------------------------------|
| <b>snmp-server contact</b> | Sets the system contact information. |

**Platform Description** N/A

## 1.18 snmp-server logging

Use this command to enable the system to log the GET, GET-NETX and SET operations of NMS.

Use the **no** form of this command to disable the SNMP logging function.

**snmp-server logging** { **get-operation** | **set-operation** }

**no snmp-server logging** { **get-operation** | **set-operation** }

| Parameter Description | Parameter            | Description                                           |
|-----------------------|----------------------|-------------------------------------------------------|
|                       | <b>get-operation</b> | Logging function for the GET and GET-NEXT operations. |
|                       | <b>set-operation</b> | Logging function for the SET operation.               |

**Defaults** The SNMP logging function is enabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command is used to enable the logging function for the GET, GET-NETX and SET operations of NMS.

With the **get-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID during the GET and GET-NEXT operations.

With the **set-operation** enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID and related values during the SET operation.

A larger number of logs may affect the device performance. Under normal condition, it is recommended to disable the SNMP logging function.

**Configuration Examples** The following example enables the logging function for the GET and SET operations:

```
Hostname(config)#snmp-server logging get-operation
Hostname(config)#snmp-server logging set-operation
```

The operation logs are displayed as below:

```
Hostname#*Feb 7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7)
operation(GET) object(id=1.3.6.1.2.1.1.5.0)

Hostname#*Feb 7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7)
operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0)

Hostname#*Feb 7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7)
operation(SET) object(id=1.3.6.1.2.1.1.5.0, value= Hostname)
```

The following example disables the logging function for the GET and SET operations:

```

Hostname(config)#no snmp-server logging get-operation
Hostname(config)#no snmp-server logging set-operation
    
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

### 1.19 snmp-server net-id

Use this command to configure the network element coding information of the device. Use the **no** form of this command to remove the network element coding information.

**snmp-server net-id** *text*  
**no snmp-server net-id**

**Parameter Description**

| Parameter   | Description                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>text</i> | Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces. |

**Defaults** No network element coding information is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the network element coding text to FZ\_CDMA\_MSC1.

```

Hostname(config)# snmp-server net-id FZ_CDMA_MSC1
    
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.20 snmp-server packetsize

Use this command to specify the largest size of the SNMP packet. Use the **no** form of this command to restore the default value.

**snmp-server packetsize** *byte-count*

**no snmp-server packetsize**

| Parameter Description | Parameter         | Description                                        |
|-----------------------|-------------------|----------------------------------------------------|
|                       | <i>byte-count</i> | Packet size. The range is from 484 to 17,876 bytes |

**Defaults** The default is 1,472 bytes.

**Command mode** Global configuration mode.

**Usage Guide** The following example specifies the largest size of SNMP packet as 1,492 bytes:

```
Hostname(config)# snmp-server packetsize 1492
```

**Configuration Examples** N/A

| Related Commands | Command                         | Description                                                        |
|------------------|---------------------------------|--------------------------------------------------------------------|
|                  | <b>snmp-server queue-length</b> | Specifies the length of the message queue for each SNMP trap host. |

**Platform** N/A

**Description**

## 1.21 snmp-server queue-length

Use this command to specify the length of the message queue for each SNMP trap host. Use the **no** form of this command to restore the default value.

**snmp-server queue-length** *length*

**no snmp-server queue-length**

| Parameter Description | Parameter     | Description                                |
|-----------------------|---------------|--------------------------------------------|
|                       | <i>length</i> | Queue length. The range is from 1 to 1000. |

**Defaults** The default is 100.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.

**Configuration Examples** The following example specifies the length of message queue as 10.

```
Hostname(config)# snmp-server queue-length 10
```

| Related Commands | Command                       | Description |
|------------------|-------------------------------|-------------|
|                  | <b>snmp-server packetsize</b> |             |

**Platform Description** N/A

## 1.22 snmp-server system-shutdown

Use this command to enable the SNMP message reload function. Use the **no** form of this command to disable the SNMP message reload function.

**snmp-server system-shutdown**  
**no snmp-server system-shutdown**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The SNMP message reload function is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.

**Configuration Examples** The following example enables the SNMP message reload function:

```
Hostname(config)# snmp-server system-shutdown
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.23 snmp-server trap-format private

Use this command to configure the SNMP traps with private fields. Use the **no** form of this command to restore the default trap format.

**snmp-server trap-format private**  
**no snmp-server trap-format private**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** The private field is not carried in the SNMP trap by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to RUIJIE-TRAP-FORMAT-MIB.mib file.  
 This command does not work if the traps are sent with SNMPv1.

**Configuration** The following example configures the SNMP trap format with the private field.

**Examples**

```
Hostname(config)# snmp-server trap-format private
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A  
**Description**

## 1.24 snmp-server trap-source

Use this command to specify the source interface of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-source interface**  
**no snmp-server trap-source**



| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>interface</i></td> <td>Specifies the source interface of the SNMP trap messages.</td> </tr> </tbody> </table> | Parameter | Description | <i>interface</i> | Specifies the source interface of the SNMP trap messages. |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|------------------|-----------------------------------------------------------|
| Parameter                    | Description                                                                                                                                                                                                              |           |             |                  |                                                           |
| <i>interface</i>             | Specifies the source interface of the SNMP trap messages.                                                                                                                                                                |           |             |                  |                                                           |
| <b>Defaults</b>              | By default, the IP address of the interface from which the SNMP packet is sent is just the source address.                                                                                                               |           |             |                  |                                                           |
| <b>Command mode</b>          | Global configuration mode.                                                                                                                                                                                               |           |             |                  |                                                           |
| <b>Usage Guide</b>           | For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.                                                                                                   |           |             |                  |                                                           |

**Configuration Examples** The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message:

```
Hostname(config)# snmp-server trap-source gigabitethernet 0/1
```

| <b>Related Commands</b>         | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>snmp-server enable traps</b></td> <td>Enables t the SNMP agent to send the SNMP trap message to NMS.</td> </tr> <tr> <td><b>snmp-server host</b></td> <td>Specifies the NMS host to send the SNMP trap message.</td> </tr> </tbody> </table> | Command | Description | <b>snmp-server enable traps</b> | Enables t the SNMP agent to send the SNMP trap message to NMS. | <b>snmp-server host</b> | Specifies the NMS host to send the SNMP trap message. |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------|---------------------------------|----------------------------------------------------------------|-------------------------|-------------------------------------------------------|
| Command                         | Description                                                                                                                                                                                                                                                                                                                                           |         |             |                                 |                                                                |                         |                                                       |
| <b>snmp-server enable traps</b> | Enables t the SNMP agent to send the SNMP trap message to NMS.                                                                                                                                                                                                                                                                                        |         |             |                                 |                                                                |                         |                                                       |
| <b>snmp-server host</b>         | Specifies the NMS host to send the SNMP trap message.                                                                                                                                                                                                                                                                                                 |         |             |                                 |                                                                |                         |                                                       |

**Platform** N/A  
**Description**

## 1.25 snmp-server trap-timeout

Use this command to define the retransmission timeout time of the SNMP trap message. Use the **no** form of this command to restore the default value.

**snmp-server trap-timeout** *seconds*

**no snmp-server trap-timeout**

| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>seconds</i></td> <td>Timeout of retransmit the SNMP trap message (in 10 milliseconds). The range is from 1 to 1,000.</td> </tr> </tbody> </table> | Parameter | Description | <i>seconds</i> | Timeout of retransmit the SNMP trap message (in 10 milliseconds). The range is from 1 to 1,000. |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|----------------|-------------------------------------------------------------------------------------------------|
| Parameter                    | Description                                                                                                                                                                                                                                                  |           |             |                |                                                                                                 |
| <i>seconds</i>               | Timeout of retransmit the SNMP trap message (in 10 milliseconds). The range is from 1 to 1,000.                                                                                                                                                              |           |             |                |                                                                                                 |

**Defaults** The default is 300 milliseconds.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies the timeout period as 60 seconds.

**Examples**

```
Hostname(config)# snmp-server trap-timeout 60
```

**Related  
Commands**

| Command                         | Description                                                   |
|---------------------------------|---------------------------------------------------------------|
| <b>snmp-server queue-length</b> | Specifies the length of message queue for the SNMP trap host. |
| <b>snmp-server host</b>         | Specifies the NMS host to send the SNMP trap message.         |
| <b>snmp-server trap-source</b>  | Specifies the source address of the SNMP trap message.        |

**Platform** N/A

**Description**

## 1.26 snmp-server udp-port

Use this command to specify a port to receive SNMP packets. Use the **no** form of this command to restore the default setting.

**snmp-server udp-port** *port-number*

**no snmp-server udp port**

**Parameter  
Description**

| Parameter          | Description                                                                       |
|--------------------|-----------------------------------------------------------------------------------|
| <i>port-number</i> | Specifies a port to receive the SNMP packets. The value range is from 1 to 65535. |

**Defaults** The default is 161.

**Command  
mode** Global configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies port 15000 to receive the SNMP packets.

**Examples**

```
Hostname(config)# snmp-server udp-port 15000
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 1.27 snmp-server user

Use this command to configure a new user to an SNMP group. Use the **no** form of this command to remove a user from an SNMP group.

**snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [ **encrypted** ] [ **auth** { **md5** | **sha** } *auth-password* ] [ **priv** **des56** *priv-password* ] } [ **access** { [ **ipv6** *ipv6\_aclname* ] *aclnum* | *aclname* } ]

**no snmp-server user** *username groupname* { **v1** | **v2c** | **v3** }

**Parameter Description**

| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>username</i>                    | Name of the user on the host that connects to the agent.                                                                                                                                                                                                                                                                                                                                                                                             |
| <i>groupname</i>                   | Name of the group to which the user belongs.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>v1</b>   <b>v2c</b>   <b>v3</b> | Specifies the SNMP version. But only SNMPv3 supports the following security parameters.                                                                                                                                                                                                                                                                                                                                                              |
| <b>encrypted</b>                   | Specifies whether the password appears in cipher text.<br>In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has 16 bytes, the SHA authentication key has 20 bytes, the SHA256 authentication key has 32 bytes, and the SHA512 authentication key has 64 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch. |
| <b>auth</b>                        | Specifies which authentication level should be used.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>md5</b>                         | Enables MD5 authentication.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>sha</b>                         | Indicates SHA.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <i>auth-password</i>               | Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.                                                                                                                                                                                                                                                                                       |
| <b>priv</b>                        | Encryption mode. des56 refers to 56-bit DES encryption protocol.                                                                                                                                                                                                                                                                                                                                                                                     |

|                      |                                                                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <i>priv-password</i> : password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key. |
| <i>priv-password</i> | Password for encryption (no more than 32 characters).                                                                                                             |
| <i>aclnumber</i>     | Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.                                                                      |
| <i>aclname</i>       | Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.                                                                 |
| <i>ipv6_aclname</i>  | Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.                                                            |

**Defaults** No user is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Hostname(config)# snmp-server user user-2 mib2user v3 auth md5 authpasstr
priv des56 despasstr
```

The following example creates an SNMPv3 user in interaction mode and configures MD5 as an authentication protocol DES and DES as an encryption protocol.

```
Hostname(config)# snmp-server user mib2user mib2group v3 interactive auth md5 priv
des56
Please configure the authentication password (1-32)
Enter Password:*****
Confirm Password:*****

Please configure the privacy password (1-32)
Enter Password:*****
Confirm Password:*****
```

**Related Commands**

| Command               | Description                           |
|-----------------------|---------------------------------------|
| <b>show snmp user</b> | Displays the SNMP user configuration. |

**Platform Description** N/A

## 1.28 snmp-server view

Use this command to configure an SNMP view. Use the **no** form of this command to remove an SNMP view.

**snmp-server view** *view-name oid-tree* { **include** | **exclude** }

**no snmp-server view** *view-name* [ *oid-tree* ]

| Parameter Description | Parameter        | Description                                             |
|-----------------------|------------------|---------------------------------------------------------|
|                       | <i>view-name</i> | View name                                               |
|                       | <i>oid-tree</i>  | Specifies the MIB object to associate with the view.    |
|                       | <b>include</b>   | Includes the sub trees of the MIB object in the view.   |
|                       | <b>exclude</b>   | Excludes the sub trees of the MIB object from the view. |

**Defaults** By default, a view is set to access all MIB objects.

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).

```
Hostname(config)# snmp-server view mib2 1.3.6.1 include
```

| Related Commands | Command               | Description                           |
|------------------|-----------------------|---------------------------------------|
|                  | <b>show snmp view</b> | Displays the SNMP view configuration. |

**Platform Description** N/A

# 1 RMON Commands

## 1.1 rmon alarm

Use this command to monitor a MIB variable. Use the **no** form of this command to remove the alarm entry.

**rmon alarm** *number variable interval {absolute | delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner ownname]*  
**no rmon alarm** *number*

| Parameter description | Parameter                      | Description                                                                                                                                                                                                      |
|-----------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>number</i>                  | Alarm number. The value ranges from <b>1</b> to <b>65535</b> .                                                                                                                                                   |
|                       | <i>variable</i>                | Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1). |
|                       | <i>interval</i>                | Sampling interval. The value ranges from <b>1</b> to <b>2147483647</b> in the unit of second.                                                                                                                    |
|                       | <b>absolute</b>                | Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.                                                                                                 |
|                       | <b>delta</b>                   | Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.                                                                   |
|                       | <b>rising-threshold value</b>  | Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from <b>-2147483648</b> to <b>+2147483647</b> .                                                          |
|                       | <i>event-number</i>            | The event number ranges from <b>1</b> to <b>65535</b> .                                                                                                                                                          |
|                       | <b>falling-threshold value</b> | Falling threshold and the corresponding event number when the threshold is reached. The threshold ranges from <b>-2147483648</b> to <b>+2147483647</b> .                                                         |
|                       | <b>owner ownname</b>           | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.                                                                                                     |

**Default** N/A.

**Command mode** Global configuration mode.

**Usage guidelines** The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

**Examples** The example below monitors the MIB variable instance ifInNUcastPkts.6.

```

Hostname(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta
rising-threshold 20 1 falling-threshold 10 1 owner zhangsan
    
```

**Related commands**

| Command                                                                                                                                                  | Description               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| <b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ]<br><b>description</b> <i>string</i> [ <b>owner</b> <i>owner-string</i> ] | Adds an event definition. |

## 1.2 rmon collection history

Use this command to enable history statistics on the Ethernet interface. Use the **no** form of this command to remove the history entry.

**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]

**no rmon collection history** *index*

**Parameter description**

| Parameter                              | Description                                                                                                                      |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <i>index</i>                           | Index of a history entry. The value ranges from <b>1</b> to <b>65535</b> .                                                       |
| <b>owner</b><br><i>ownername</i>       | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.                     |
| <b>buckets</b><br><i>bucket-number</i> | Capacity of a history entry. The value ranges from <b>1</b> to <b>65535</b> . The default value is 10.                           |
| <b>interval</b><br><i>seconds</i>      | Statistics period. The unit is second. The value ranges from <b>1</b> to <b>3600</b> . The default value is <b>1800</b> seconds. |

**Default**

N/A.

**Command mode**

Interface configuration mode.

**Usage guidelines**

The configured history control entry parameters cannot be modified. And the history entry cannot be removed from the interface where the entry configured.

**Examples**

The example below enables log statistics on interface GigabitEthernet 0/1.

```

Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-GigabitEthernet0/1)#rmon collection history 1 owner
UserA buckets 5 interval 60
    
```

**Related commands**

| Command                                                                         | Description                                         |
|---------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>rmon collection stats</b> <i>index</i><br>[ <b>owner</b> <i>owner-name</i> ] | Adds a statistical entry on the Ethernet interface. |

## 1.3 rmon collection stats

Use this command to monitor an Ethernet interface. Use the **no** form of this command to remove the configuration.

**rmon collection stats** *index* [**owner** *owner-string*]

**no rmon collection stats** *index*

| Parameter description | Parameter                     | Description                                                                                                                            |
|-----------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>index</i>                  | Index of the statistic table. The value ranges from <b>1</b> to <b>65535</b> .                                                         |
|                       | <b>owner</b> <i>ownername</i> | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces. |

**Default** N/A.

**Command mode** Interface configuration mode.

**Usage guidelines** The configured history control entry parameters cannot be modified. And the history entry cannot be removed from the interface where the entry configured.

The example below enables monitoring the statistics of interface GigabitEthernet 0/1.

### Examples

```

Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#interface gigabitEthernet 0/1
Hostname(config-GigabitEthernet0/1)# rmon collection stats 1 owner
UserA

```

| Related commands | Command                                                                                                                                                     | Description                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                  | <b>rmon collection history</b> <i>index</i> [ <b>owner</b> <i>owner-name</i> ]<br><b>[buckets</b> <i>bucket-number</i> ] [ <b>interval</b> <i>seconds</i> ] | Adds a history control entry. |

## 1.4 rmon event

Use this command to define an event. Use the **no** form of this command to remove the event entry.

**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *owner-name*]

**no rmon event** *number*

| Parameter description | Parameter     | Description                                                         |
|-----------------------|---------------|---------------------------------------------------------------------|
|                       | <i>number</i> | Event number. The value ranges from <b>1</b> to <b>65535</b> .      |
|                       | <b>log</b>    | Log event. When a log event is triggered, the system records a log. |



|                                                 |                                                                                                              |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>trap</b> <i>community</i>                    | Trap event. When a trap event is triggered, the system sends trap with the group named “community”.          |
| <b>description</b><br><i>description-string</i> | Description of the event. The value is a character string consisting of 1 to 127 characters.                 |
| <b>owner</b> <i>owner-name</i>                  | Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive. |

**Default** N/A.

**Command mode** Global configuration mode.

**Usage guidelines** The RGOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.

The example below defines the event actions: log event and send trap message.

**Examples**

```

Hostname#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#rmon event 1 log trap public description
"ifInNUcastPkts is abnormal" owner UserA
    
```

**Related commands**

| Command                                                                                                                                                              | Description          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon alarm</b> <i>number variable interval {absolute   delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]</i> | Adds an alarm entry. |

## 1.5 show rmon

**Default** Use this command to display the RMON configuration.

**show rmo**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the RMON configuration.

**Examples**

```

Hostname#show rmon
ether statistic table:
    index = 1
    
```

```
interface = GigabitEthernet 0/1
owner = admin
status = 0
dropEvents = 61
octets = 170647461
pkts = 580375
broadcastPkts = 2135
multiPkts = 3615
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

rmon history control table:

```
index = 1
interface = GigabitEthernet 0/1
bucketsRequested = 5
bucketsGranted = 5
interval = 60
owner = UserA
stats = 1
```

rmon history table:

```
index = 1
sampleIndex = 2485
intervalStart = 7d:22h:56m:38s
dropEvents = 0
octets = 5840
pkts = 27
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
```

```

        collisions = 0
        utilization = 0
rmon alarm table:
        index: 1
        interval: 60
        oid = 1.3.6.1.2.1.2.2.1.12.6
        sampleType: 2
        alarmValue: 0
        startupAlarm: 3
        risingThreshold: 20
        fallingThreshold: 10
        risingEventIndex: 1
        fallingEventIndex: 1
        owner: UserA
        status: 1

rmon event table:
        index = 1
        description = ifInNUcastPkts is abnormal
        type = 4
        community = public
        lastTimeSent = 0d:0h:0m:0s
        owner =UserA
        status = 1

rmon log table:
        eventIndex = 1
        index = 1
        logTime = 6 d:19 h:21 m:48 s
        logDescription = ifInNUcastPkts is abnormal
    
```

**Related commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

## 1.6 show rmon alarm

- Default** Use this command to display the RMON alarm table.  
**show rmon alarm**
- Default** N/A.
- Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the RMON alarm table.

**Examples**

```

Hostname#show rmon alarm
rmon alarm table:
      index: 1
      interval: 60
      oid = 1.3.6.1.2.1.2.2.1.12.6
      sampleType: 2
      alarmValue: 0
      startupAlarm: 3
      risingThreshold: 20
      fallingThreshold: 10
      risingEventIndex: 1
      fallingEventIndex: 1
      owner: UserA
      status: 1
    
```

**Related commands**

| Command                                                                                                                                                                                                                                              | Description          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon alarm</b> <i>number variable</i><br><i>interval {absolute   delta }</i><br><b>rising-threshold</b> <i>value</i><br><i>[event-number]</i> <b>falling-threshold</b> <i>value</i><br><i>[event-number]</i> [ <b>owner</b><br><i>ownername</i> ] | Adds an alarm entry. |

## 1.7 show rmon event

Use this command to display the event configuration.

**show rmon event**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

**Examples**

The example below displays the event configuration.

```

Hostname#show rmon event
rmon event table:
      index = 1
      description = ifInNUcastPkts is abnormal
      type = 4
    
```

```

community = public
lastTimeSent = 0d:0h:0m:0s
owner =UserA
status = 1

rmon log table:
eventIndex = 1
index = 1
logTime = 6d:19h:21m:48s
logDescription = ifInNUcastPkts is abnormal
    
```

**Related commands**

| Command                                                                                                                                                            | Description          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>rmon event</b> <i>number</i> [ <b>log</b> ] [ <b>trap</b> <i>community</i> ] [ <b>description</b> <i>description-string</i> ] [ <b>owner</b> <i>ownername</i> ] | Adds an event entry. |

## 1.8 show rmon history

Use this command to display the history information.

**show rmon history**

**Default** N/A.

**Command mode** Privileged EXEC mode.

**Usage guidelines** N/A.

The example below displays the history information.

**Examples**

```

Hostname#show rmon history
rmon history control table:
index = 1
interface = GigabitEthernet 0/1
bucketsRequested = 5
bucketsGranted = 5
interval = 60
owner = UserA
stats = 1

rmon history table:
index = 1
sampleIndex = 2485
intervalStart = 7d:22h:56m:38s
dropEvents = 0
octets = 5840
    
```

```

pkts = 27
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0
    
```

**Related commands**

| Command                                                                                                                                                    | Description                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <b>rmon collection history</b> <i>index</i><br>[ <i>owner ownername</i> ] [ <b>buckets</b><br><i>bucket-number</i> ] [ <b>interval</b><br><i>seconds</i> ] | Adds a history control entry. |

### 1.9 show rmon statistics

Use this command to display the RMON statistics.

**show rmon statistics**

**Default**

N/A.

**Command mode**

Privileged EXEC mode.

**Usage guidelines**

N/A.

The example below displays the RMON statistics.

**Examples**

```

Hostname#show rmon statistics
ether statistic table:
    index = 1
    interface = GigabitEthernet 0/1
    owner = admin
    status = 0
    dropEvents = 61
    octets = 170647461
    pkts = 580375
    broadcastPkts = 2135
    multiPkts = 3615
    crcAlignErrors = 0
    underSizePkts = 0
    overSizePkts = 0
    
```

```
fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865
```

**Related  
commands**

| Command                                                                        | Description               |
|--------------------------------------------------------------------------------|---------------------------|
| <b>rmon collection stats</b> <i>index</i> [ <b>owner</b> <i>owner-string</i> ] | Adds a statistical entry. |

# 1 CWMP Commands

## 1.1 acs password

Use this command to configure the ACS password to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to cancel the configuration.

**acs password** { *password* | *encryption-password* *encrypted-password* }



**no acs password**

| Parameter Description | Parameter                  | Description                                                                                                                                    |
|-----------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>password</i>            | Configures the ACS user password to be authenticated for the CPE to connect to the ACS.                                                        |
|                       | <i>encryption-password</i> | Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used). |
|                       | <i>encrypted-password</i>  | Specifies the password in encrypted form.                                                                                                      |

**Defaults**  
*encryption-password*: 0  
*encrypted-password*: N/A

**Command Mode**  
 CWMP configuration mode

**Usage Guide** Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

-  The command contains English letters in upper or lower case and numeric characters.
-  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

**Configuration Examples** The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs password 123
Hostname(config-cwmp)#

```



| Related Commands | Command                        | Description                                                                        |
|------------------|--------------------------------|------------------------------------------------------------------------------------|
|                  | <b>show cwmp configuration</b> | Displays the current configuration of CWMP.                                        |
|                  | <b>show cwmp status</b>        | Displays the running status of CWMP.                                               |
|                  | <b>acs username</b>            | Configures the ACS username to be authenticated for the CPE to connect to the ACS. |

**Platform** N/A  
**Description**

## 1.2 acs url

Use this command to configure the URL of the ACS to which the CPE will connect.

Use the **no** form of this command to restore the default setting.

**acs url** *url*

**no acs url**

| Parameter Description | Parameter  | Description                   |
|-----------------------|------------|-------------------------------|
|                       | <i>url</i> | Specifies the URL of the ACS. |

**Defaults** N/A

**Command Mode** CWMP configuration mode

**Usage Guide** Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements:

- The URL of the ACS is formatted as `http://ip [: port ]/ path`.
- The URL of the ACS consists of at most 255 characters.

**Configuration Examples** The following example specifies the URL of the ACS to `http://10.10.10.1:7547/acs`.

```

Hostname#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs url http://10.10.10.1:7547/acs
Hostname(config-cwmp)#

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|------------------|---------|-------------|

|                                |                                             |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A

**Description**

### 1.3 acs username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the **no** form of this command to restore the default setting.

**acs username** *username*

**no acs username**

**Parameter Description**

| Parameter       | Description                                                                        |
|-----------------|------------------------------------------------------------------------------------|
| <i>username</i> | Configures the ACS username to be authenticated for the CPE to connect to the ACS. |

**Defaults** N/A

**Command** CWMP configuration mode

**Mode**

**Usage Guide** Configures the ACS username to be authenticated for the CPE to connect to the ACS.

**Configuration Examples** The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#acs username admin
Hostname(config-cwmp)#

```

**Related Commands**

| Command                        | Description                                                                        |
|--------------------------------|------------------------------------------------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP.                                        |
| <b>show cwmp status</b>        | Displays the running status of CWMP.                                               |
| <b>acs password</b>            | Configures the ACS password to be authenticated for the CPE to connect to the ACS. |

**Platform** N/A

**Description**

## 1.4 cpe back-up

Use this command to configure the backup and restoration of the main program and configuration file of the CPE.

Use the **no** form of this command to disable this function.

**cpe back-up** [ **delay-time** *seconds* ]

**no cpe back-up**

### Parameter Description

| Parameter      | Description                                                                                                                                                |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>seconds</i> | Specifies the delay for backup and restoration of the main program and configuration file of the CPE, in the range from 30 to 1,000 in the unit of seconds |

### Defaults

The default is 60 seconds.

### Command Mode

CWMP configuration mode

### Usage Guide

You can configure the restoration function on a CPE, so that the CPE can restore itself from exceptions of its main program or configuration file. Then when the CPE fails to connect to the ACS and breaks away from the NMS after its main program or configuration file is upgraded, the previous main program or configuration file of the CPE can be restored in time for the ACS to manage the CPE. This kind of exception is generally caused by delivery of a wrong main program or configuration file.

### Configuration Examples

The following example disables the backup and restoration of the main program and configuration file of the CPE.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#no cpe back-up
Hostname(config-cwmp)#

```

### Related Commands

| Command                        | Description                                 |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

### Platform

N/A

### Description

## 1.5 cpe inform

Use this command to configure the periodic notification function of the CPE.

Use the **no** form of this command to restore the default setting

**cpe inform** [ *interval seconds* ] [ *start-time time* ]

**no cpe inform**

| Parameter Description | Parameter      | Description                                                                                                     |
|-----------------------|----------------|-----------------------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds. |
|                       | <i>time</i>    | Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.                 |


**Defaults** The default is 600 seconds.

**Command** CWMP configuration mode

**Mode**

**Usage Guide** Use this command to configure the periodic notification function of the CPE.

- If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval.
- If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.

 The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.

**Configuration** The following example specifies the periodical notification interval of the CPE to 60 seconds.

**Examples**

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe inform interval 60
Hostname(config-cwmp)#
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|------------------|---------|-------------|

|                                |                                             |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A

**Description**

## 1.6 cpe password

Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the **no** form of this command to cancel the configuration.

**cpe password** { *password* | *encryption-password* *encrypted-password* }

**no cpe password**

**Parameter Description**

| Parameter                  | Description                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>password</i>            | Configures the CPE user password to be authenticated for the ACS to connect to the CPE.                                                        |
| <i>encryption-password</i> | Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used). |
| <i>encrypted-password</i>  | Specifies the password in encrypted form.                                                                                                      |

**Defaults**

*encryption-password*: 0

*encrypted-password*: N/A



**Command**

CWMP configuration mode

**Mode**

**Usage Guide**

Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:

-  Contain 1 to 26 characters including uppercase letters, lowercase letters, and digits.
-  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.

**Configuration Examples**

The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe password 123
Hostname(config-cwmp)#
    
```

**Related  
Commands**

| Command                        | Description                                                                        |
|--------------------------------|------------------------------------------------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP.                                        |
| <b>show cwmp status</b>        | Displays the running status of CWMP.                                               |
| <b>acs username</b>            | Configures the CPE username to be authenticated for the ACS to connect to the CPE. |

**Platform** N/A  
**Description**

## 1.7 cpe url

Use this command to configure the URL of the CPE to which the ACS will connect.

Use the **no** form of this command to restore default setting.

**cpe url** *url*

**no cpe url**

**Parameter  
Description**

| Parameter  | Description                                                        |
|------------|--------------------------------------------------------------------|
| <i>url</i> | Specifies the URL of the CPE in the string of 1 to 256 Characters. |

**Defaults** N/A

**Command  
Mode** CWMP configuration mode

**Usage Guide** ●

**Configuration** The following example specifies the URL of the CPE to `http://10.10.10.1:7547/acs`.

**Examples**

```

Hostname#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/
Hostname(config-cwmp)#

```

**Related  
Commands**

| Command                        | Description                                 |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A  
**Description**

## 1.8 cpe username

Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS.

Use the **no** form of this command to restore the default setting.

**cpe username** *username*

**no cpe username**

**Parameter**  
**Description**

| Parameter       | Description                                                                        |
|-----------------|------------------------------------------------------------------------------------|
| <i>username</i> | Configures the CPE username to be authenticated for the ACS to connect to the CPE. |

**Defaults** N/A

**Command** CWMP configuration mode  
**Mode**

**Usage Guide** Configures the CPE username to be authenticated for the ACS to connect to the CPE.

**Configuration Examples** The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwp
Hostname(config-cwp)#cpe username admin
Hostname(config-cwp)#

```

**Related**  
**Commands**

| Command                       | Description                                                                        |
|-------------------------------|------------------------------------------------------------------------------------|
| <b>show cwp configuration</b> | Displays the current configuration of CWMP.                                        |
| <b>show cwp status</b>        | Displays the running status of CWMP.                                               |
| <b>cpe password</b>           | Configures the CPE password to be authenticated for the ACS to connect to the CPE. |

**Platform** N/A  
**Description**

## 1.9 cwmp

Use this command to enable the CWMP function.

Use the **no** form of this command to disable this function.

**cwmp**

**no cwmp**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |

**Defaults** By default, this function is enabled.

**Command Mode** Global configuration mode

**Usage Guide** Use this command to enable or disable the CWMP function.

**Configuration Examples** The following example disables the CWMP function.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#no cwmp
Hostname(config)#
    
```

| <b>Related Commands</b> | Command                        | Description                                 |
|-------------------------|--------------------------------|---------------------------------------------|
|                         | <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
|                         | <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform Description** N/A

## 1.10 disable download

Run the **disable download** command to disable the management function of receiving any main program and configuration file delivered by the ACS.

Use the **no** form of this command to restore the default setting.

**disable download**

**no disable download**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |



**Defaults** By default, the CPE can download main program and configuration files from the ACS.

**Command Mode** CWMP configuration mode

**Usage Guide** The **disable download** command is used to disable the management function of receiving any main program and configuration file delivered by the ACS.

- This command is invalid for configuration script files. That is, when this command is used, the configuration script can still be executed.

**Configuration Examples** The following example disables the management function of receiving any main program and configuration file delivered by the ACS.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#disable download
Hostname(config-cwmp)#

```

**Related Commands**

| Command                        | Description                                 |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A

**Description**

## 1.11 disable upload

Run the **disable upload** command to disable the management function of uploading any main program, configuration file, and log file to the ACS.

Use the **no** form of this command to restore the default setting.

**disable upload**

**no disable upload**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** By default, the CPE can upload its configuration and log files to the ACS.

**Command Mode** CWMP configuration mode

**Usage Guide** Disable the management function of uploading any main program, configuration file, and log file to the ACS.

**Configuration Examples** The following example disables the management function of uploading any main program, configuration file and log file to the ACS.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#disable upload
Hostname(config-cwmp)#
    
```

**Related Commands**

| Command                        | Description                                 |
|--------------------------------|---------------------------------------------|
| <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
| <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A

**Description**

## 1.12 show cwmp configuration

Use this command to display the current configuration of CWMP.

**show cwmp configuration**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privilege EXEC mode

**Usage Guide**

**Configuration Examples** The following example displays the current configuration of CWMP.

```

Hostname(config-cwmp)#show cwmp configuration
CWMP Status           : enable
ACS URL                : http://www.Hostname.com.cn/acs
ACS username          : admin
ACS password           : *****
CPE URL                : http://10.10.10.2:7547/
CPE username           : Hostname
    
```

```

CPE password           : *****
CPE inform status      : disable
CPE inform interval    : 60s
CPE inform start time  : 0:0:0 0 0 0
CPE wait timeout       : 50s
CPE download status    : enable
CPE upload status      : enable
CPE back up status     : enable
CPE back up delay time : 60s
    
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

| Field                  | Description                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------|
| CWMP Status            | Running status of CWMP.                                                                         |
| ACS URL                | URL of the ACS.                                                                                 |
| ACS username           | ACS username to be authenticated for the CPE to connect to the ACS.                             |
| ACS password           | ACS password to be authenticated for the CPE to connect to the ACS.                             |
| CPE URL                | URL of the CPE.                                                                                 |
| CPE username           | CPE username to be authenticated for the ACS to connect to the CPE.                             |
| CPE password           | CPE password to be authenticated for the ACS to connect to the CPE.                             |
| CPE inform status      | Status of CPE periodical notification function.                                                 |
| CPE inform interval    | CPE periodical notification interval.                                                           |
| CPE wait timeout       | Timeout period of CPE sessions.                                                                 |
| CPE inform start time  | The start time of periodical notification.                                                      |
| CPE download status    | Indicates whether to download main program and configuration files from the ACS.                |
| CPE upload status      | Whether to upload any main program and configuration file and log file to the ACS               |
| CPE back up status     | Indicates whether backup and restoration of the main program and configuration file is enabled. |
| CPE back up delay time | Delay time of the backup and restoration of the main program and configuration files.           |

**Related Commands**

| Command                 | Description                          |
|-------------------------|--------------------------------------|
| <b>show cwmp status</b> | Displays the running status of CWMP. |

**Platform** N/A  
**Description**

### 1.13 show cwmp status

Uses this command to display the running status of CWMP

**show cwmp status**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays the running status of CWMP.

```

Examples
Hostname#show cwmp status
CWMP Status           : enable
Session status        : Close
Last success session   : Unknown
Last success session time : Thu Jan 1 00:00:00 1970
Last fail session      : Unknown
Last fail session time : Thu Jan 1 00:00:00 1970
Session retry times    : 0
    
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

| Field                     | Description                                                   |
|---------------------------|---------------------------------------------------------------|
| CWMP Status               | The running status of CWMP                                    |
| Session status            | The current status of the session between the CPE and the ACS |
| Last success session      | The last success session type                                 |
| Last success session time | The last success session time                                 |
| Last fail session         | The last failed session type                                  |
| Last fail session time    | The last failed session time                                  |
| Session retry times       | The number of session retransmission attempts                 |

| Related Commands | Command                        | Description                                 |
|------------------|--------------------------------|---------------------------------------------|
|                  | <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |

**Platform Description** N/A

## 1.14 stun max-period

Uses this command to configure the maximum STUN keepalive interval.

**stun max-period** *interval*

**no stun max-period**

| Parameter Description | Parameter       | Description                                                                                         |
|-----------------------|-----------------|-----------------------------------------------------------------------------------------------------|
|                       | <i>interval</i> | Configures the maximum STUN keepalive interval, in the range from 0 to 3600 in the unit of seconds. |

**Defaults** The default maximum STUN keepalive interval is 60 seconds.

**Command** CWMP configuration mode

**Mode**

**Usage Guide** Use this command to configure the maximum STUN keepalive interval.

**Configuration** The following example sets the maximum STUN keepalive interval to 80 seconds.

**Examples**

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# stun max-period 80
Hostname(config-cwmp)#

```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.15 stun min-period

Uses this command to configure the minimum STUN keepalive interval.

**stun min-period** *interval*

**no stun min-period**

| Parameter Description | Parameter       | Description                                                                                         |
|-----------------------|-----------------|-----------------------------------------------------------------------------------------------------|
|                       | <i>interval</i> | Configures the minimum STUN keepalive interval, in the range from 0 to 3600 in the unit of seconds. |

**Defaults** The default minimum STUN keepalive interval is 20 seconds.

**Command** CWMP configuration mode

**Mode**

**Usage Guide** Use this command to configure the minimum STUN keepalive interval.

**Configuration** The following example sets the minimum STUN keepalive interval to 80 seconds.

**Examples**

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# stun min-period 80
Hostname(config-cwmp)#

```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.16 stun port

Uses this command to configure the STUN server port.

**stun port** *port-number*

**no stun port**

**Parameter  
Description**

| Parameter          | Description                                                           |
|--------------------|-----------------------------------------------------------------------|
| <i>port-number</i> | Configures the STUN server port number, in the range from 0 to 65535. |

**Defaults** The default STUN server port is 3478.

**Command** CWMP configuration mode

**Mode**

**Usage Guide** Use this command to configure the STUN server port.

**Configuration** The following example sets the STUN server port to 3479.

**Examples**

```

Hostname> enable
Hostname# configure terminal

```

```

Hostname(config)# cwmp
Hostname(config-cwmp)# stun port 3479
Hostname(config-cwmp)#
    
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A  
**Description**

### 1.17 timer cpe-timeout

Uses this command to configure the session timeout period of the CPE.

**timer cpe-timeout** *seconds*  
**no timer cpe-timeout**

| Parameter Description | Parameter | Description    |
|-----------------------|-----------|----------------|
|                       |           | <i>seconds</i> |

**Defaults** By default, the session timeout period is 30 seconds.

**Command Mode** CWMP configuration mode

**Usage Guide** Use this command to configure the session timeout period of the CPE.  
 The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.

**Configuration Examples** The following example configures the session timeout period of the CPE to 50 seconds.

```

Hostname#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)#cwmp
Hostname(config-cwmp)#timer cpe-timeout 50
Hostname(config-cwmp)#
    
```

| Related Commands | Command                        | Description                                 |
|------------------|--------------------------------|---------------------------------------------|
|                  | <b>show cwmp configuration</b> | Displays the current configuration of CWMP. |
|                  | <b>show cwmp status</b>        | Displays the running status of CWMP.        |

**Platform** N/A  
**Description**



## VPN Commands

---

1. PPP Commands
2. IPsec Commands
3. PPPoE Client Commands



# 1 PPP Commands

## 1.1 ppp accm

Use this command to configure the Asynchronous Control Character Map (ACCM) option for PPP negotiation.

**ppp accm** *value*

Use the **no** form of this command to restore the default setting.

**no ppp accm**

| Parameter Description | Parameter    | Description                                                  |
|-----------------------|--------------|--------------------------------------------------------------|
|                       | <i>value</i> | Value of the ACCM option, in the range from 0 to 0xffffffff. |

Command Mode Interface configuration mode

Defaults The default is 0x000A0000.

Default Level 14

Usage Guide This command is used to configure the ACCM option involved in the PPP negotiation phase, in the range from 0 to 0xffffffff. The default is 0x000A0000.

Configuration Examples The following example configures the ACCM option for PPP negotiation.

```

Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)#ppp accm 0x0000000f
    
```

Verification Run the **show running-config** command to display the value of the ACCM option configured on the current interface for PPP negotiation.

Note N/A

Platform N/A

## 1.2 ppp authentication

Use this command to configure the authentication mode of PPP.

```
ppp authentication { { chap | ms-chap | ms-chap-v2 | pap } * [ callin | default | list-name ] }
```

Use the **no** form of this command to delete the authentication mode of PPP.

```
no ppp authentication { { chap | ms-chap | ms-chap-v2 | pap } * [ callin | default | list-name ] }
```

Parameter  
Description

| Parameter         | Description                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------|
| <b>pap</b>        | Sets the authentication mode to PAP.                                                        |
| <b>callin</b>     | Authenticates incoming request packets only.                                                |
| <b>chap</b>       | Sets the authentication mode to CHAP.                                                       |
| <b>default</b>    | Uses the default authentication list, no matter whether PAP or CHAP authentication applies. |
| <i>list_name</i>  | Configures the name of the authentication list.                                             |
| <b>ms-chap</b>    | Sets the authentication mode to ms-chap.                                                    |
| <b>ms-chap-v2</b> | Sets the authentication mode to ms-chap-v2.                                                 |

Command  
Mode

Interface configuration mode

Default Level

14

Usage Guide

This command is used to configure the authentication mode of PPP, which may be PAP or CHAP authentication.

Configuration

The following example configures the authentication mode of PPP.

Examples

```
Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)#ppp authentication pap
Hostname(config-if-Virtual-ppp 1)#ppp authentication chap
Hostname(config-if-Virtual-ppp 1)#ppp authentication pap chap callin default
Hostname(config-if-Virtual-ppp 1)#ppp authentication pap chap test-list
```

Verification

Run the **show running-config** command to display whether the authentication mode of PPP has been configured on the current interface.

Note

N/A

Common

N/A

Error

Platform

N/A

### 1.3 ppp chap

The following example configures the user name and password for CHAP authentication of PPP.

```
ppp chap hostname name
ppp chap password password
```

Use the **no** form of this command to delete the configured user name and password for CHAP authentication of PPP.

```
no ppp chap hostname
```

| Parameter Description | Parameter       | Description                       |
|-----------------------|-----------------|-----------------------------------|
|                       | <i>name</i>     | User name for CHAP authentication |
|                       | <i>password</i> | Password for CHAP authentication  |

Command Mode Interface configuration mode

Default Level 14

Usage Guide PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for CHAP authentication.

Configuration Examples The following example configures the user name and password for CHAP authentication on interface Virtual-PPP 1.

```
Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)#ppp chap hostname 111
Hostname(config-if-Virtual-ppp 1)# ppp chap password 111
```

Verification Run the **show running-config** command to display the user name and password configured on the current interface for CHAP authentication.

Note N/A

Common Error N/A

Platform N/A

## 1.4 ppp ipcp dns

Use this command to configure the DNS option involved in the IPCP phase of PPP negotiation.

**ppp ipcp dns** { *A.B.C.D* [ *A.B.C.D* ] [ **accept** ] | **accept** | **request** | **reject** }

Use this command to delete the configured DNS option.

**no ppp ipcp dns** { *A.B.C.D* [ *A.B.C.D* ] [ **accept** ] | **accept** | **request** | **reject** }

Parameter  
Description

| Parameter      | Description                                            |
|----------------|--------------------------------------------------------|
| <b>accept</b>  | Receives all non-0 DNS addresses.                      |
| <b>request</b> | Requests the DNS address from the peer server.         |
| <b>reject</b>  | Refuses to negotiate the DNS option with the peer end. |
| <i>A.B.C.D</i> | DNS address                                            |

Defaults The DNS option is not configured by default.

Command Mode Interface configuration mode

Default Level 14

Usage Guide This command is used to configure the DNS option involved in the IPCP negotiation phase.

Configuration Examples The following example configures the DNS option involved in the IPCP negotiation phase.

```

Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)#ppp ipcp dns accept
Hostname(config-if-Virtual-ppp 1)#ppp ipcp dns reject
Hostname(config-if-Virtual-ppp 1)#ppp ipcp dns request
Hostname(config-if-Virtual-ppp 1)# ppp ipcp dns 1.1.1.1 2.2.2.2
    
```

Verification Run the **show running-config** command to display whether the DNS option has been configured on the current interface.

Note N/A

Common Error N/A

Platform N/A

## 1.5 ppp lcp mru negotiate

Use this command to configure the Maximum Receive Unit (MRU) option for PPP auto-negotiation.

**ppp lcp mru negotiate**

Use the no form of this command to remove the MRU configuration.

**no ppp lcp mru**

| Parameter Description         | Parameter                                                                                                                                                                                                                     | Description |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                               | N/A                                                                                                                                                                                                                           | N/A         |
| <b>Command Mode</b>           | Interface configuration mode                                                                                                                                                                                                  |             |
| <b>Default Level</b>          | 14                                                                                                                                                                                                                            |             |
| <b>Usage Guide</b>            | The MRU option, as a common option involved in the PPP negotiation process, will be carried in packets from both ends during negotiation so as to determine the maximum size of packets to be transmitted on the entire link. |             |
| <b>Configuration Examples</b> | The following example configures the MRU option for auto-negotiation on interface Virtual-ppp 1.                                                                                                                              |             |
|                               | <pre> Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)#ppp lcp mru negotiate </pre>                                                                                   |             |
| <b>Verification</b>           | 1. Run the <b>show running-config</b> command to display whether the MRU option has been configured on the current interface.                                                                                                 |             |
| <b>Note</b>                   | N/A                                                                                                                                                                                                                           |             |
| <b>Common Error</b>           | N/A                                                                                                                                                                                                                           |             |
| <b>Platform</b>               | N/A                                                                                                                                                                                                                           |             |

## 1.6 ppp max-bad-auth

Use this command to specify the number of PPP authentication retries.

**ppp max-bad-auth** *number*

Use the **no** form of this command to restore the default setting.

**no ppp max-bad-auth**

| Parameter Description  | Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Description                                                      |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
|                        | <i>number</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Number of PPP authentication retries, in the range from 1 to 255 |
| Defaults               | The default is 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                  |
| Command Mode           | Interface configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                  |
| Default Level          | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                  |
| Usage Guide            | The number of PPP authentication retries includes the first authentication; that is, if the number of PPP authentication retries is set to 3, twice authentication is still allowed following the failure of the first authentication. When the last authentication fails, the line is interrupted (or reset).                                                                                                                                                                                         |                                                                  |
| Configuration Examples | <p>The following example sets the number of PPP authentication retries on interface virtual-ppp1 to 3:</p> <pre> Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)# ppp max-bad-auth 3 </pre> <p>The following example restores the number of PPP authentication retries to the default setting.</p> <pre> Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)# no ppp max-bad-auth </pre> |                                                                  |
| Verification           | Run the <b>show running-config interface virtual-ppp 1</b> command to display the configuration on the current interface.                                                                                                                                                                                                                                                                                                                                                                              |                                                                  |
| Note                   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                  |
| Common Error           | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                  |
| Platform               | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                  |

## 1.7 ppp pap sent-username *password*

Use this command to configure the user name and password for PAP authentication of PPP.

**ppp pap sent-username** *username password password*

Use the **no** form of this command to delete the configured user name and password for PAP authentication of PPP.

**no ppp pap sent-username**

| Parameter<br>Description  | Parameter                                                                                                                                                                                                                             | Description                      |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
|                           | <i>username</i>                                                                                                                                                                                                                       | User name for PAP authentication |
|                           | <i>password</i>                                                                                                                                                                                                                       | Password for PAP authentication  |
| Command<br>Mode           | Interface configuration mode                                                                                                                                                                                                          |                                  |
| Default Level             | 14                                                                                                                                                                                                                                    |                                  |
| Usage Guide               | PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for PAP authentication. |                                  |
| Configuration<br>Examples | The following example configures the user name and password for PAP authentication on interface Virtual-PPP 1.                                                                                                                        |                                  |
|                           | <pre> Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)# ppp pap sent-username 111 password 111 </pre>                                                                         |                                  |
| Verification              | Run the <b>show running-config</b> command to display the user name and password configured on the current interface for PAP authentication.                                                                                          |                                  |
| Note                      | N/A                                                                                                                                                                                                                                   |                                  |
| Common<br>Error           | N/A                                                                                                                                                                                                                                   |                                  |
| Platform                  | N/A                                                                                                                                                                                                                                   |                                  |

## 1.8 ppp negotiation-timeout

Use this command to specify the maximum PPP negotiation timeout period.

**ppp negotiation-timeout** *seconds*

Use the **no** form of this command to restore the default setting.

**no ppp negotiation-timeout**

| Parameter<br>Description | Parameter      | Description                                                                                  |
|--------------------------|----------------|----------------------------------------------------------------------------------------------|
|                          | <i>seconds</i> | Maximum PPP negotiation timeout period, in the range from 10 to 65535 in the unit of seconds |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>               | The default is 20 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Command Mode</b>           | Interface configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default Level</b>          | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Usage Guide</b>            | If the maximum negotiation timeout period expires but PPP negotiation is not finished, the PPP negotiation is considered as having failed. The maximum PPP negotiation timeout period is 20s by default.                                                                                                                                                                                                                                                                                                                          |
| <b>Configuration Examples</b> | <p>The following example sets the maximum PPP negotiation timeout period on interface virtual-ppp1 to 200 seconds.</p> <pre>Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)# ppp negotiation-timeout 200</pre> <p>The following example restores the maximum PPP negotiation timeout period to the default settings.</p> <pre>Hostname# configure terminal Hostname(config)# interface virtual-ppp 1 Hostname(config-if-Virtual-ppp 1)# no ppp negotiation-timeout</pre> |
| <b>Verification</b>           | Run the <b>show running-config interface virtual-ppp 1</b> command to check the configuration on the current interface.                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Note</b>                   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Common Error</b>           | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Platform</b>               | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



# 1 IPSEC-IKE Commands

## 15.1 IPsec authentication (IKE policy)

Use this command to specify the authentication method for IKE policies.

**authentication [ pre-share ]**

Use the **no** form of this command to restore the default configuration.

**no authentication**

| Parameter Description | Parameter        | Description                              |
|-----------------------|------------------|------------------------------------------|
|                       | <b>pre-share</b> | Indicates pre-shared key authentication. |

**Defaults** The pre-shared key authentication is used by default.

**Command Mode** IKE policy configuration mode

**Default Level** 14

**Usage Guide**  IKE negotiation policies use the pre-shared key authentication by default.

**Configuration Example** Configure an IKE policy with the priority of 10 and use pre-shared key authentication in the policy.

```
Hostname(config)# crypto isakmp policy 10
Hostname(isakmp-policy)#authentication pre-share
```

Configure an IKE policy with the priority of 10 and use digital envelop authentication SM2.

```
Hostname(config)# crypto isakmp policy 10
Hostname(isakmp-policy)#authentication digital-email asymmetric sm2
```

**Verification** N/A

## 15.2 clear crypto isakmp

Use this command to clear the currently running IKE security association (SA).

**clear crypto isakmp [ connection-id ]**

| Parameter Description | Parameter            | Description                                                        |
|-----------------------|----------------------|--------------------------------------------------------------------|
|                       | <i>connection-id</i> | Indicates the ID of an IKE SA. All existing IKE SAs are cleared by |

|  |                                              |
|--|----------------------------------------------|
|  | default. The value range is from 0 to 65535. |
|--|----------------------------------------------|

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** In general, only a specific IKE SA is cleared. Run the **show crypto isakmp sa** command to display the ID of the SA to be cleared, and then run the **clear crypto isakmp** command using the ID to clear the specific IKE SA.

**Configuration** #Clear all IKE SAs.

**Example** Hostname# clear crypto isakmp

## 15.3 clear crypto sa

Use this command to clear an IPsec SA.

**clear crypto sa**

Use this command to clear an IPsec SA of the remote peer by IP address or host name.

**clear crypto sa peer** { *ip-address* | *peer-name* }

Use this command to clear an IPsec SA of the remote peer by encryption mapping name.

**clear crypto sa map** *map-name*

Use this command to clear an IPsec SA of the remote peer by IP address and security parameter index (SPI).

**clear crypto sa spi** *destination-address* { **ah** | **esp** } *spi*

**Parameter Description**

| Parameter                  | Description                                                   |
|----------------------------|---------------------------------------------------------------|
| <i>ip-address</i>          | Indicates the IP address of the remote peer.                  |
| <i>peer-name</i>           | Indicates the host name of the remote peer.                   |
| <i>map-name</i>            | Indicates the name of an encryption mapping set.              |
| <i>destination-address</i> | Indicates the IP address of the local or remote peer.         |
| <i>spi</i>                 | Specifies an SPI. The value range is from 0 to 4,294,967,295. |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** 1. The preceding commands are used to clear IPsec SAs. If the **peer**, **map**, and **SPI** keywords are not specified, all IPsec SAs will be deleted by default.

2. If an SA is established via IKE, the SA will be cleared. If IPSec activation packets are detected on an interface, IPSec renegotiates a new SA. If an SA is manually configured, the SA will be cleared and a new SA will be re-established.
3. New parameters are effective only to SAs negotiated after the parameter configuration but do not affect existing SAs. To make new parameters effective to existing SAs, run commands to clear existing SAs for SA re-negotiation.
4. The deletion of SAs will interrupt communication. To ensure that communication using other IPSec SAs is not interrupted, use the **peer**, **map**, and **SPI** keywords to specify a specific SA.
5. If only one SA is available or no data is communicated through other SAs, clear all SAs for SA re-negotiation.

**Configuration** #Clear all IKE SAs.

**Example** Hostname# clear crypto sa

## 15.4 crypto dynamic-map

Use this command to create a dynamic encryption mapping entry and enter the encryption mapping configuration mode.

**crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num*

Use the **no** form of this command to delete an encryption mapping set or entry.

**no crypto dynamic-map** *dynamic-map-name* [*dynamic-seq-num*]

| Parameter Description | Parameter               | Description                                                                           |
|-----------------------|-------------------------|---------------------------------------------------------------------------------------|
|                       | <i>dynamic-map-name</i> | Specifies the name of an encryption mapping set.                                      |
|                       | <i>dynamic-seq-num</i>  | Specifies the ID of an encryption mapping entry. The value range is from 1 to 65,535. |

**Defaults** No dynamic encryption mapping exists by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide**

**Configuration**

**Example**

**Verification** N/A

## 15.5 crypto ipsec df-bit

Use this command to set the DF value of the encapsulation header for all interfaces.

**crypto ipsec df-bit { clear | set | copy }**


| Parameter Description | Parameter    | Description                                                                                                                             |
|-----------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>clear</b> | Zeroes out the DF bit in the external IP header. The device may fragment packets and encapsulate the data via IPsec.                    |
|                       | <b>set</b>   | Sets the DF bit to 1 in the external IP header. If the DF bit in the original IP header is zeroed out, the device may fragment packets. |
|                       | <b>copy</b>  | Uses the original DF bit value as the DF bit value in the external header. The default value is <b>copy</b> .                           |

**Defaults** This command is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** In IPsec tunnel mode, use the **clear** keyword in the command when you need to send packets with the size greater than the MTU or when you do not know the size of the MTU.

 If this command is not enabled using a specific parameter, the device uses **copy** as the DF bit value by default.

**Configuration** #Zero out the DF bit of all interfaces.

**Example**

```
Hostname(config)# crypto ipsec df-bit clear
```

**Verification** N/A

## 15.6 crypto ipsec multicast disable

Use this command to disable IPsec processing on multicast and broadcast packets.

**crypto ipsec multicast disable**

Use the **no** form of this command to enable IPsec processing on multicast and broadcast packets.

**no crypto ipsec multicast disable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

|                      |                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>      | When this command is not configured and an ACL involves multicast and broadcast packets, the device conducts IPsec processing on the packets by default. |
| <b>Command Mode</b>  | Global configuration mode                                                                                                                                |
| <b>Default Level</b> | 14                                                                                                                                                       |
| <b>Usage Guide</b>   | If IPsec processing is not required for multicast and broadcast packets, configure this command to skip IPsec processing.                                |
| <b>Configuration</b> | #Disable IPsec processing on multicast and broadcast packets.                                                                                            |
| <b>Example</b>       | <pre>Hostname(config)# crypto ipsec multicast disable</pre>                                                                                              |
| <b>Verification</b>  | N/A                                                                                                                                                      |

## 15.7 crypto ipsec optional

Use this command to disable the IPsec security check.

**crypto ipsec optional**

Use the **no** form of this command to enable the IPsec security check.

**no crypto ipsec optional**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |

|                      |                                                                                                                                                                                                                                                                                                                               |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>      | IPsec security check is enabled by default.                                                                                                                                                                                                                                                                                   |
| <b>Command Mode</b>  | Global configuration mode                                                                                                                                                                                                                                                                                                     |
| <b>Default Level</b> | 14                                                                                                                                                                                                                                                                                                                            |
| <b>Usage Guide</b>   | The security check consumes considerable resources. Disabling the security check can save CPU resources. In the L2TP over IPsec model, the IPsec security check can be forcibly enabled or only IPsec encrypted packets are allowed to pass through. For example, L2TP and IPsec encryption may be used together as required. |
| <b>Configuration</b> | Cancel security check.                                                                                                                                                                                                                                                                                                        |
| <b>Example</b>       | <pre>Hostname(config)# crypto ipsec optional</pre>                                                                                                                                                                                                                                                                            |
| <b>Verification</b>  | N/A                                                                                                                                                                                                                                                                                                                           |

## 15.8 crypto ipsec profile ( global ipsec-profile )

Use this command to create or modify an encryption mapping set (profile).

**crypto ipsec profile** *profile-name*

Use the **no** form of this command to cancel an encryption mapping set (profile) or entry.

**no crypto ipsec profile** *profile-name*

| Parameter<br>Description | Parameter           | Description                                                |
|--------------------------|---------------------|------------------------------------------------------------|
|                          | <i>profile-name</i> | Indicates the name of an encryption mapping set (profile). |

**Defaults** No encryption mapping set is configured by default.

**Command Mode** Global configuration mode  
Run this command to enter the profile encryption mapping configuration mode.

**Default Level** 14

**Usage Guide** When data encryption and protection are required on a tunnel interface, define an encryption mapping set (profile) and then apply it to the tunnel interface. Define encryption communication parameters in the encryption mapping set (profile). The parameters include the following:

1. IPsec security policies to be applied to communication: Select policies from the list composed of one or more transformation sets.
2. SA lifetime
3. Information about whether SAs are manually configured or established via IKE
4. ACLs that support **permit any** for negotiation in the case of IPv6, IPsec-IPv4, and IPsec-IPv6 tunnels

Apply the encryption mapping set of a tunnel to the tunnel interface. In this way, all IP communication through the tunnel interface will be encrypted according to the encryption mapping set applied to the tunnel interface. After configuration is completed, the device automatically initiates IKE negotiation, or triggers IKE negotiation when receiving packets from this interface. Policies described in encryption mapping entries are used during SA negotiation. To ensure smooth IPsec communication between two IPsec peers, the encryption mapping entries of the tunnel between the two peers must contain compatible configuration statements. When two peers try to establish an SA, each of the peers must have one encryption mapping entry compatible with one encryption mapping entry of the other peer, and the encryption mapping entry must meet at least the following conditions:

1. An encryption mapping entry must contain a compatible encryption access list (for example, image access list).
2. Encryption mapping entries of both peers must specify the peer address (unless the peer is using a dynamic encryption set).
3. The encryption mapping entries must share at least one identical transformation set.
4. Only one encryption mapping set is applied to a single interface. The encryption mapping set specifies IPsec/IKE.

Create multiple encryption mapping entries for one interface in either of the following cases:

1. Different data flows of the interface will be processed by different IPSec peers.
2. Different levels of IPSec security need to be applied to different types of communication (data sent to the same or different peers), for example, the communication between devices in one subnet needs to be authenticated while the communication between devices in another subnet needs to be authenticated and encrypted. In this case, different types of communication should be defined in two different ACLs, and one separate encryption mapping entry must be created for each encryption access list.

**Configuration Example** #Complete the minimum configuration for an encryption mapping set (profile). The name of the profile is testprofile and the name of the transformation set is mytest.

```

Hostname(config)# crypto ipsec profile testprofile
Hostname(config-crypto-map)# set transform-set myset

```

**Verification** N/A

## 15.9 crypto ipsec security-association detect

Use this command to configure an IPSec SA detection interval.

**crypto ipsec security-association detect** *second*

Use the **no** form of this command to delete the configured IPSec SA detection interval.

**no crypto ipsec security-association detect** *second*

| Parameter Description | Parameter     | Description                                                                |
|-----------------------|---------------|----------------------------------------------------------------------------|
|                       | <i>second</i> | Specifies the IPSec SA detection interval. The value ranges from 5 to 100. |

**Defaults** IPSec SA detection is not enabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** IPSec SA detection is not enabled by default. When data cannot be forwarded over an existing IPSec tunnel, re-negotiation cannot be performed. After this command is configured, you can check whether data forwarding is normal. If data fails to be forwarded, IPSec SA re-negotiation is performed again.

**Configuration Example** Set the IPSec SA detection interval to 30s.

```

Hostname(config)# crypto ipsec security-association detect 30

```

**Verification** -

|                      |   |
|----------------------|---|
| Notifications        | - |
| Common Errors        | - |
| Platform Description | - |

## 15.10 crypto ipsec security-association expire-time

Use this command to change the expiration time of an old IPSec security association after a new association is negotiated.

**crypto ipsec security-association expire-time** *second*

Use the **no** form of this command to restore the default value.

**no crypto ipsec security-association lifetime** *second*

| Parameter Description | Parameter                                                                                                                                                                                 | Description                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
|                       | <i>second</i>                                                                                                                                                                             | Ranges from 1 to 60. The default value is 30. |
| Defaults              | 30 seconds                                                                                                                                                                                |                                               |
| Command Mode          | Global configuration mode                                                                                                                                                                 |                                               |
| Default Level         | 14                                                                                                                                                                                        |                                               |
| Usage Guide           | By default, the old IPSec security association works for 30 seconds after a new association is negotiated. You can run this command to modify the expiration time of the old association. |                                               |
| Configuration Example | #Set the expiration time to 10.<br><pre>Hostname(config)#crypto ipsec security-association expire-time 10</pre>                                                                           |                                               |
| Verification          | N/A                                                                                                                                                                                       |                                               |

## 15.11 crypto ipsec security-association lifetime

Use this command to change the global lifetime of an IPSec SA.

**crypto ipsec security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes* }

Use the **no** form of this command to restore the default value of lifetime.

**no crypto ipsec security-association lifetime** { **seconds** *seconds* | **kilobytes** *kilobytes* }



| Parameter Description | Parameter                         | Description                                                                                                                                                                                                                                                      |
|-----------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>seconds</b> <i>seconds</i>     | Indicates the SA timeout period in seconds. The default value is 3,600 (1 hour). It can be set to <b>0</b> , indicating that the timeout function is disabled. The value can be <b>0</b> , or any value from 120 to 86,400.                                      |
|                       | <b>kilobytes</b> <i>kilobytes</i> | Indicates the timeout communication amount of an SA in kilobytes. The default value is <b>4,608,000</b> . It can be set to <b>0</b> , indicating that the byte timeout function is disabled. The value can be <b>0</b> , or any value from 2,560 to 536,870,912. |

**Defaults** 3,600 seconds (1 hour) and 4,608,000 KB (communication for 1 hour at the rate of 10 MB per second)

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide**

- The communication encrypted using IPsec SAs uses shared keys. An SA times out after a period of time is reached or a certain communication amount is reached, so as to ensure security. Both ends need to re-negotiate an SA and use the new shared key. When devices negotiate an SA, the smaller value between the lifetime proposed by the peer and that configured on the local device is used as the lifetime of the new SA.
- There are two lifetimes: time lifetime and communication amount lifetime. An SA times out whenever either lifetime expires first. If the global lifetime is changed, this change is effective only to new SAs that are negotiated after the change and does not affect existing SAs. To make the new settings take effect as soon as possible, run the **clear crypto sa** command to clear some or all content in the SA database.
- To change the global time lifetime, run the **crypto IPsec security-association lifetime seconds** command. The time lifetime specifies that an SA times out after certain seconds. To change the global communication amount lifetime, run the **crypto IPsec security-association lifetime kilobytes** command. The communication amount lifetime specifies that an SA times out when the amount (in KB) of communication encrypted using the SA key reaches a certain amount.
- A smaller lifetime indicates a lower probability of successful key cracking, because there is less data that is encrypted using the same key and that can be used by attackers for analysis. However, when the lifetime is shorter, it takes longer time for the CPU to establish a new SA. Manually configured SAs does not involve lifetime.
- Lifetime work principle: After a certain period of time (specified by **seconds**) is reached or a certain data communication amount (specified by the **kilobytes** keyword) is reached, whichever is earlier, an SA (and relevant key) will time out. The negotiation of a new SA starts before the old SA lifetime expires. In this way, a new SA is available before the old SA times out. The negotiation of a new SA starts 30 seconds before the lifetime specified by the **seconds** keyword times out or 256 KB away from the amount lifetime of data communication carried by the tunnel (specified by the **kilobytes** keyword) expires, whichever is earlier. If no communication passes through a tunnel within the lifetime of an SA, no new SA will be negotiated when the SA times out. Likewise, the negotiation of a new SA starts only when IPsec needs to protect a packet.

- The time lifetime and communication amount lifetime cannot be zero simultaneously. Otherwise, the negotiation will fail. The device does not check the local configuration and you need to confirm that the time lifetime and communication amount lifetime are not zero simultaneously.

**Configuration Example** #Set the time lifetime to 2,500 seconds and communication amount lifetime to 2,304,000 KB (communication for half an hour at the rate of 10 MB) for IPsec SAs.

```

Hostname(config)# crypto ipsec security-association lifetime seconds 2500
Hostname(config)# crypto ipsec security-association lifetime kilobytes 2304000

```

**Verification** N/A

## 15.12 crypto ipsec security-association lifetime not\_based\_on initiator

Use this command to modify the negotiation match rule for lifetime in Phase 2 of IPsec. That is, the final negotiation result of lifetime in Phase 2 is the smaller value between the lifetime of the device in branch and that of the device in the headquarters.

**crypto ipsec security-association lifetime not\_based\_on initiator**

Use the **no** form of this command to restore the default match rule of lifetime in Phase 2. That is, the final negotiation result uses the lifetime of the device in the branch.

**no crypto ipsec security-association lifetime { seconds | kilobytes }**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The final negotiation result of lifetime in Phase 2 uses the lifetime of the device in the branch by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** By default, the negotiation result of lifetime in Phase 2 uses the lifetime of the device in the branch, indicating that devices in both the headquarters and the branch use the lifetime of the branch as the lifetime in Phase 2. You can use the command to modify the match rule of the lifetime in Phase 2, so as to use the smaller value between the lifetime of the device in the headquarters and that of the device in the branch as the final negotiation result.

**Configuration Example** #Modify the match result of lifetime in Phase 2.

```

Hostname(config)# crypto ipsec security-association lifetime not_based_on
initiator

```

**Verification** N/A

## 15.13 crypto ipsec security-association replay disable

Use this command to disable the replay function so as not to check retransmitted packets.

**crypto ipsec security-association replay disable**

Use the **no** form of this command to check retransmitted packets.

**no crypto ipsec security-association replay disable**

| <b>Parameter Description</b> | Parameter                                                                                                                                                                          | Description |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                              | N/A                                                                                                                                                                                | N/A         |
| <b>Defaults</b>              | Replay check is enabled by default. This command is not configured by default.                                                                                                     |             |
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                          |             |
| <b>Default Level</b>         | 14                                                                                                                                                                                 |             |
| <b>Usage Guide</b>           | After the command is executed to disable replay, packet retransmission is not checked, which can improve packet processing efficiency but increase the possibility of DoS attacks. |             |
| <b>Configuration Example</b> | #Disable the packet retransmission check.                                                                                                                                          |             |
| <b>Example</b>               | <pre> Hostname(config)# crypto ipsec security-association replay disable </pre>                                                                                                    |             |
| <b>Verification</b>          | N/A                                                                                                                                                                                |             |

## 15.14 crypto ipsec transform-set

Use this command to define a transformation set for SAs.

**crypto ipsec transform-set** *transform-set-name* *transform1* [*transform2* [*transform3* ]]

Use the **no** form of this command to delete a transformation set.

**no crypto ipsec transform-set** *transform-set-name*

| <b>Parameter Description</b> | Parameter                                                    | Description                                                                                                     |
|------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|                              | <i>transform-set-name</i>                                    | Indicates the name of a transformation set.                                                                     |
|                              | <i>transform1</i> , <i>transform2</i> ,<br><i>transform3</i> | Indicates the security protocol and algorithm used by an SA. For details, see the security configuration guide. |

**Defaults** No transformation set is configured by default.

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Default Level</b>         | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Usage Guide</b>           | <ol style="list-style-type: none"> <li>1. A set is a combination of security protocols, algorithms, and other settings for communication protected by IPsec. During IPsec SA negotiation, peers must use the same specific transformation set to protect specific data flows.</li> <li>2. Configure multiple transformation sets and then specify one or more of them in encryption mapping entries. Transformation sets defined in encryption mapping entries are used for IPsec SA negotiation, so as to protect data flows that match the ACL referenced in the encryption mapping entries. During negotiation, both peers search for the same transformation set that is available on both peers. When such a transformation set is found, it is selected as a part of IPsec SAs of both peers and applied to protected communication.</li> <li>3. If an SA is configured manually, no parameter needs to be negotiated for the SA. Therefore, the same transformation set must be specified on both peers.</li> </ol> |
| <b>Configuration Example</b> | <p>#Define a transformation set that uses the ESP-DES-MD5 protection mode (providing encryption and authentication services).</p> <pre>Hostname(config)# crypto ipsec transform-set myset esp-des esp-md5-hmac</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Verification</b>          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## 15.15 crypto isakmp aggressive-encrypt enable

Use this command to enable encryption for the third packet used in the negotiation in aggressive mode.

**crypto isakmp aggressive-encrypt enable**

Use the **no** form of this command to restore default settings.

**no crypto isakmp aggressive-encrypt enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** Encryption is enabled for the third packet used in the negotiation in aggressive mode by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** When the device interconnects to a partner's device, the device checks whether the third packet is encrypted for the negotiation in aggressive mode. If it is not encrypted, the negotiation fails. Therefore, encryption is enabled for the third packet by default. If encryption is not required in some scenarios, you can run the **no crypto isakmp aggressive-encrypt enable** command to disable this function.

**Configuration** #Configure encryption for the third packet used in the negotiation in aggressive mode.

**Example** `Hostname(config)# crypto isakmp aggressive-encrypt enable`

**Verification** Run the **show running-config** command to display the configuration.

**Prompts** N/A

**Common Errors** N/A

**Platform** N/A

**Description**

## 15.16 crypto isakmp enable

Use this command to enable IKE so as to use IKE to negotiate IPsec SAs.

**crypto isakmp enable**

Use the **no** form of this command to disable IKE.

**no crypto isakmp enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** IKE is enabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** IKE is enabled by default. If you need to use IKE for IPsec SA negotiation, this command is not required. If you do not use IKE for IPsec SA negotiation, use the **no** form of this command to disable IKE.

**Configuration** #Enable IKE.

**Example** `Hostname(config)# crypto isakmp enable`

**Verification** N/A

## 15.17 crypto isakmp key

Use this command to specify the pre-shared key used in IKE negotiation.

**crypto isakmp key { 0 | 7 } keystring { hostname peer-hostname | address peer-address [ mask ] }**

Use the **no** form of this command to delete the specified pre-shared key.

**no crypto isakmp key { 0 | 7 } kestring { hostname peer-hostname | address peer-address [ mask ] }**

| Parameter Description | Parameter            | Description                                                                                                              |
|-----------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------|
|                       | <b>0   7</b>         | Specifies a plaintext key or ciphertext key. <b>0</b> indicates a plaintext key and <b>7</b> indicates a ciphertext key. |
|                       | <i>kestring</i>      | Indicates the pre-shared key string. It can contain a maximum of 128 characters.                                         |
|                       | <i>peer-hostname</i> | Indicates the host name of the remote peer.                                                                              |
|                       | <i>peer-address</i>  | Indicates the IP address of the remote peer.                                                                             |
|                       | <i>mask</i>          | Specifies the subnet for a network segment address.                                                                      |

**Defaults** No pre-shared key is specified by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** In general, IKE uses a pre-shared key for negotiation. To enable IKE to successfully establish an IKE SA, use this command to configure the same pre-shared key on both communication peers. If the specified peer is a network segment, use **mask** to identify the subnet mask. When both **peer-address** and **Mask** are **0.0.0.0**, the default pre-shared key is used.

**Configuration Example** #Set the pre-shared key used for IKE negotiation with the peer at the IP address of 172.16.1.1 to **mysecret**.

```
Hostname(config)# crypto isakmp key 0 mysecret address 172.16.1.1
```

**Verification** N/A

## 15.18 crypto isakmp keepalive

Use this command to send peer detection messages to the remote peer.

**crypto isakmp keepalive secs [ on-demand | periodic ]**

**crypto isakmp keepalive secs retries [ on-demand | periodic ]**

Use the **no** form of this command to disable the peer detection function.

**no crypto isakmp keepalive**

| Parameter Description | Parameter   | Description                                                              |
|-----------------------|-------------|--------------------------------------------------------------------------|
|                       | <i>secs</i> | Indicates the keepalive duration of a tunnel in seconds. The value range |

|                  |                                                                                                |
|------------------|------------------------------------------------------------------------------------------------|
|                  | is from 5 to 3600.                                                                             |
| <i>retries</i>   | Indicates the interval for retransmitting packets in seconds. The value range is from 2 to 60. |
| <b>on-demand</b> | Sends messages at the idle time of packet forwarding.                                          |
| <b>periodic</b>  | Sends messages at the configured interval.                                                     |

**Defaults** No peer detection message is sent by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use the **crypto isakmp keepalive** command to enable the device to periodically send peer detection messages to the remote peer, to check whether the remote peer is alive.  
On-demand detection: when forwarding the packet, the device will send detection messages if does not receive packet after the specified time.

**Configuration Example** #Set the tunnel keepalive duration to 60 seconds, packet retransmission interval to 5 seconds, and use the on-demand mode.

```
Hostname(config)# crypto isakmp keepalive 60 5 on-demand
```

**Verification** N/A

## 15.19 crypto isakmp limit disable

Use this command to disable the speed limit of IKE negotiation.

**crypto isakmp limit disable**

Use the **no** form of this command to enable the speed limit of IKE negotiation.

**no crypto isakmp limit disable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The speed limit of IKE negotiation is enabled by default. The negotiation speed is 1000.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** The command is used to disable the speed limit of IKE negotiation.

**Configuration** The following example disables the speed limit of IKE negotiation.

**Example**

```
Hostname(config)# crypto isakmp limit disable
```

**Verification** N/A

## 15.20 crypto isakmp limit rate

Use this command to limit the speed of IKE negotiation.

**crypto isakmp limit rate** *numbers*

Use the **no** form of this command to restore the default settings.

**no crypto isakmp limit rate**

| Parameter Description | Parameter | Description   |
|-----------------------|-----------|---------------|
|                       | numbers   | Limited speed |

**Defaults** The negotiation speed is 1000 by default, that is, 1000 IPSec tunnels negotiate at the same time.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** The negotiation may not converge or be slow if thousands of tunnels negotiate at the same time, so that the process may take hours. The command is used to limit the tunnel quantity in the specified range to improve the negotiation efficiency.

**Configuration** The following example configures the negotiation speed of IKE.

**Example**

```
Hostname(config)# crypto isakmp limit rate 500
```

**Verification** N/A

## 15.21 crypto isakmp mode-detect

Use this command to enable the local security gateway to automatically use the aggressive mode for negotiation when it fails to complete IKE negotiation initiated by the peer in main mode.

**crypto isakmp mode-detect**

Use the **no** form of this command to disable the automatic aggressive mode.

**no crypto isakmp mode-detect**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|



|                      |                                                                                                                                                                                                                                                                                                                                                                              |     |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>Description</b>   |                                                                                                                                                                                                                                                                                                                                                                              |     |
|                      | N/A                                                                                                                                                                                                                                                                                                                                                                          | N/A |
| <b>Defaults</b>      | When this command is not configured, only the main mode is adopted for negotiation by default.                                                                                                                                                                                                                                                                               |     |
| <b>Command Mode</b>  | Global configuration mode                                                                                                                                                                                                                                                                                                                                                    |     |
| <b>Default Level</b> | 14                                                                                                                                                                                                                                                                                                                                                                           |     |
| <b>Usage Guide</b>   | Many vendors set foot in security products but the implementation methods of security products from different vendors are different. Only two work modes are supported in Phase 1 of IKE negotiation. To ensure compatibility, use this command to automatically complete negotiation in aggressive mode when the IKE negotiation initiated by the peer cannot be completed. |     |
| <b>Configuration</b> | #Enable the device to automatically identify negotiation initiated in aggressive mode.                                                                                                                                                                                                                                                                                       |     |
| <b>Example</b>       | <pre>Hostname(config)# crypto isakmp mode-detect</pre>                                                                                                                                                                                                                                                                                                                       |     |
| <b>Verification</b>  | N/A                                                                                                                                                                                                                                                                                                                                                                          |     |

## 15.22 crypto isakmp nat-traversal disable

Use this command to disable the NAT traversal function.

**crypto isakmp nat-traversal disable**

Use the **no** form of this command to enable the NAT traversal function.

**no crypto isakmp nat-traversal disable**

|                              |                                                                                                                                                                                                            |                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Parameter Description</b> | <b>Parameter</b>                                                                                                                                                                                           | <b>Description</b> |
|                              | N/A                                                                                                                                                                                                        | N/A                |
| <b>Defaults</b>              | NAT traversal is enabled by default.                                                                                                                                                                       |                    |
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                                                  |                    |
| <b>Default Level</b>         | 14                                                                                                                                                                                                         |                    |
| <b>Usage Guide</b>           | The protocols for implementing the NAT traversal function supported by devices of some vendors may be incompatible. In special cases, disable the NAT traversal function to implement device interworking. |                    |
| <b>Configuration</b>         | #Disable the NAT traversal function.                                                                                                                                                                       |                    |
| <b>Example</b>               | <pre>Hostname(config)# crypto isakmp nat-traversal disable</pre>                                                                                                                                           |                    |
| <b>Verification</b>          | N/A                                                                                                                                                                                                        |                    |

## 15.23 crypto isakmp nat keepalive

Use this command to configure the interval for sending NAT keepalive messages.

**crypto isakmp nat keepalive secs**

Use the **no** form of this command to cancel the configured interval for sending NAT keepalive messages and restore the default transmission interval.

**no crypto isakmp nat keepalive**

| <b>Parameter Description</b> | Parameter                                                                                                                                                                                                                                                                                                                                                                                              | Description                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|                              | secs                                                                                                                                                                                                                                                                                                                                                                                                   | Indicates the keepalive duration of a tunnel in seconds. The value range is from 5 to 3,600. |
| <b>Defaults</b>              | The default value is 300 seconds.                                                                                                                                                                                                                                                                                                                                                                      |                                                                                              |
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                                                                                                                                                                                                                                              |                                                                                              |
| <b>Default Level</b>         | 14                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                              |
| <b>Usage Guide</b>           | The device complies with RFC3947 and uses the IPSEC NAT-T technology and UDP header to resolve the NAT traversal problem. The keepalive mode is used for transmitting packets to prevent NAT connection timeout. Run the <b>crypto isakmp nat keepalive</b> command to specify the interval for sending keepalive messages. If the interval is not specified, the default value (300 seconds) is used. |                                                                                              |
| <b>Configuration Example</b> | #Set the interval for sending tunnel keepalive packets to 60 seconds.                                                                                                                                                                                                                                                                                                                                  |                                                                                              |
| <b>Example</b>               | <pre> Hostname(config)# crypto isakmp nat keepalive 60 </pre>                                                                                                                                                                                                                                                                                                                                          |                                                                                              |
| <b>Verification</b>          | N/A                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                              |

## 15.24 crypto isakmp next-payload disable

Use this command to disable the next-payload check.

**crypto isakmp next-payload disable**

Use the **no** form of this command to enable the next-payload check.

**no crypto isakmp next-payload disable**

| <b>Parameter Description</b> | Parameter | Description |
|------------------------------|-----------|-------------|
|                              | N/A       | N/A         |

**Defaults** By default, when DOI information cannot be identified, the device considers that the negotiation cannot

continue and returns a failure message.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** After the next-payload check is disabled, the DOI field that cannot be identified is ignored and the negotiation continues. However, if the reserved field is not **0** or the field length does not match the length range, a failure message is still returned.

**Configuration** #Disable the next-payload check.

**Example**

```
Hostname(config)# crypto isakmp next-payload disable
```

**Verification** N/A

## 15.25 crypto isakmp peer

Use this command to specify the first peer that initiates negotiation in the case of multiple peers.

**crypto isakmp peer { bind | random }**

Use the **no** form of this command to cancel the priority of the specified first peer that initiates negotiation.

**no crypto isakmp peer**

| Parameter Description | Parameter     | Description                                                                                                                                                                                                                            |
|-----------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>bind</b>   | Binds peers with IPsec dialup peer addresses when multiple peer addresses are configured for a 3G card. This parameter takes effect only in 3G networks. The first dialup maps to the first peer according to the configured sequence. |
|                       | <b>random</b> | Randomly selects the first peer that tries to initiate negotiation.                                                                                                                                                                    |

**Defaults** By default, the negotiation starts from the first peer according to the configured sequence.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** When 3G links are used, if multiple dialup addresses configured for a 3G card map to peers in the IPsec mapping set, enable the peer binding function to accelerate dialup. Otherwise, the device needs to try multiple times to find the correct peer. It takes a long time to establish a tunnel for the first time.

**Configuration** #Enable the function of randomly selecting the tunnel connection address.

**Example**

```
Hostname(config)# crypto isakmp peer random
```

**Verification** N/A

## 15.26 crypto isakmp policy

Use this command to define an IKE policy of a certain priority and enter the IKE policy configuration mode.

**crypto isakmp policy** *priority*

Use the **no** form of this command to delete the policy of a certain priority.

**no crypto isakmp policy** *priority*

| Parameter Description | Parameter       | Description                                                                                                                                                                                      |
|-----------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>priority</i> | Indicates the priority of an IKE policy. The value is an integer in the range from 1 to 10,000, where <b>1</b> indicates the highest priority while <b>10,000</b> indicates the lowest priority. |

**Defaults** There is no default priority.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to specify parameters for negotiating IKE SAs. Run this command to enter the IKE policy configuration mode. In IKE policy configuration mode, you can set the following parameters:

- encryption (IKE policy): The default value is 56-bit DES-CBC.
- hash (IKE policy): The default value is SHA-1.
- authentication (IKE policy): The default value is RSA signature.
- group (IKE policy): The default value is 768-bit group.
- Diffie-Hellman lifetime(IKE policy): The default value is 86,400 seconds (1 day).

If a parameter is not set, the default value of the parameter is used. You can configure multiple IKE policies on the device. After the IKE negotiation starts, the device tries to search for the public policy configured at both ends, and the search starts from the policy with the specified highest priority on the remote peer.

**Configuration** #Configure an IKE policy with the priority of 100.

**Example**

```

Hostname(config)# crypto isakmp policy 100
Hostname(isakmp-policy)# authentication pre-share
Hostname(isakmp-policy)# encryption des
Hostname(isakmp-policy)# group 2
Hostname(isakmp-policy)# hash sha

```

**Verification** N/A

## 15.27 crypto isakmp session limit

Use this command to configure the limit on the number of IKE negotiations. The value ranges from **5** to **1024**.

**crypto isakmp session limit** *numbers*

Use the **no** form of this command to restore default settings.

**no crypto isakmp session limit** *numbers*

| Parameter Description        | Parameter                                                                                                                                                                                                                                                                                                                                            | Description                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
|                              | <i>numbers</i>                                                                                                                                                                                                                                                                                                                                       | Indicates the limit on the number of IKE negotiations. |
| <b>Defaults</b>              | The limit on the number of IKE negotiations is not configured by default.                                                                                                                                                                                                                                                                            |                                                        |
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                                                                                                                                                                                            |                                                        |
| <b>Default Level</b>         | 14                                                                                                                                                                                                                                                                                                                                                   |                                                        |
| <b>Usage Guide</b>           | After the limit on the number of IKE negotiations is configured, the maximum number of clients that are allowed to initiate IKE negotiation cannot exceed this limit. When there is a large variation in the number of users and many users request access, you need to limit the maximum number of connections to protect the performance of IPsec. |                                                        |
| <b>Configuration Example</b> | #Set the limit on the number of IKE negotiations to 10.<br><pre>Hostname(config)# crypto isakmp session limit 10</pre>                                                                                                                                                                                                                               |                                                        |
| <b>Verification</b>          | Run the <b>show running-config</b> command to check the limit on the number of IKE negotiations.                                                                                                                                                                                                                                                     |                                                        |
| <b>Prompts</b>               | N/A                                                                                                                                                                                                                                                                                                                                                  |                                                        |
| <b>Common Errors</b>         | N/A                                                                                                                                                                                                                                                                                                                                                  |                                                        |
| <b>Platform Description</b>  | N/A                                                                                                                                                                                                                                                                                                                                                  |                                                        |

## 15.28 crypto isakmp vendorid disable

Use this command to disable the transmission of Ruijie vendor ID information during IKE negotiation.

**crypto isakmp vendorid disable**

Use the **no** form of this command to enable the transmission of Ruijie vendor ID information during IKE negotiation.

**no crypto isakmp vendorid disable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** By default, Ruijie vendor ID information is transmitted during IKE negotiation.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Devices from some vendors cannot identify private vendor IDs during IKE negotiation, resulting in a negotiation failure. In this case, use this command to disable transmission of Ruijie vendor ID information.

**Configuration** #Disable transmission of vendor IDs during negotiation.

**Example** `Hostname(config)# crypto isakmp vendorid disable`

**Verification** N/A

## 15.29 crypto map (global IPsec)

Use this command to create or modify an encryption mapping set.

**crypto map** *map-name* *seq-num* { *ipsec-manual* | *ipsec-isakmp* [ *dynamic* *dynamic-map-name* ] }

Use the **no** form of this command to cancel an encryption mapping set or entry.

**no crypto map** *map-name* [ *seq-num* ]

| Parameter Description | Parameter               | Description                                                                                     |
|-----------------------|-------------------------|-------------------------------------------------------------------------------------------------|
|                       | <i>map-name</i>         | Indicates the name of an encryption mapping set.                                                |
|                       | <i>seq-num</i>          | Indicates the serial number of an encryption mapping entry. The value range is from 1 to 65535. |
|                       | <b>ipsec-manual</b>     | Specifies that a mapping entry is used for manually configuring IPsec SAs.                      |
|                       | <b>ipsec-isakmp</b>     | Specifies that a mapping entry is used for establishing IPsec SAs negotiated via IKE.           |
|                       | <i>dynamic-map-name</i> | Specifies the name of a dynamic encryption mapping set that is used as a policy template.       |

**Defaults** No encryption mapping set is configured by default.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command</b>       | Global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Mode</b>          | Run this command to enter the encryption mapping configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Default Level</b> | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Usage Guide</b>   | <p>To encrypt and protect data using IPsec, define an encryption mapping set and then apply it to a specific interface. Define encryption communication parameters in the encryption mapping set. The parameters include the following:</p> <ol style="list-style-type: none"><li>1. IPsec protection to be provided for communication: Associate a configured encryption access list.</li><li>2. Destination address of the communication protected via IPsec: Specify the remote IPsec peer.</li><li>3. Local address used for IPsec communication: Apply the encryption mapping set to an interface. IPsec uses the address of a communication interface as the address of the local peer.</li><li>4. IPsec security policies to be applied to communication: Select policies from the list composed of one or more transformation sets.</li><li>5. SA lifetime</li><li>6. Information about whether SAs are manually configured or established via IKE</li></ol> <p>Encryption mapping entries that share the same encryption mapping name but have different mapping SNs constitute one encryption mapping set. Apply the encryption mapping set to an interface. In this way, all IP communication through the interface will be checked according to the encryption mapping set applied to the interface. If outbound IP communication matches an encryption mapping entry and needs to be protected, and IKE is specified in the encryption mapping entry, the device negotiates an SA with the remote peer according to parameters specified in the encryption mapping entry. If manually configured SAs are specified in the encryption mapping entry, an SA must be configured during the configuration of the encryption mapping entry. Provided that an SA is successfully established, data will be encrypted for transmission regardless of whether the SA is manually configured or established via IKE. If the SA negotiation fails, data will be discarded.</p> <p>Policies described in encryption mapping entries are used during SA association. To ensure smooth IPsec communication between two IPsec peers, the encryption mapping entries of the two peers must contain compatible configuration statements. When two peers try to establish an SA, each of the peers must have one encryption mapping entry compatible with one encryption mapping entry of the other peer, and the encryption mapping entry must meet at least the following conditions:</p> <ol style="list-style-type: none"><li>1. An encryption mapping entry must contain a compatible encryption access list (for example, image access list).</li><li>2. Encryption mapping entries of both peers must specify the peer address (unless the peer is using a dynamic encryption mapping set).</li><li>3. The encryption mapping entries must share at least one identical transformation set.</li><li>4. Only one encryption mapping set is applied to a single interface. The encryption mapping set specifies IPsec/IKE or the combination of IPsec and manually configured entries. To create multiple encryption mapping entries for a specified interface, use the <b>seq-num</b> parameter to rank these encryption mapping entries. A smaller value of <b>seq-num</b> indicates a higher priority.</li></ol> <p>Create multiple encryption mapping entries for one interface in either of the following cases:</p> <ol style="list-style-type: none"><li>1. Different data flows of the interface will be processed by different IPsec peers.</li><li>2. Different levels of IPsec security need to be applied to different types of communication (data sent to the same or different peers), for example, the communication between devices in one subnet needs</li></ol> |

to be authenticated while the communication between devices in another subnet needs to be authenticated and encrypted. In this case, different types of communication should be defined in two different ACLs, and one separate encryption mapping entry must be created for each encryption access list.

For use of dynamic encryption mapping, see the section "crypto dynamic-map".

**Configuration** #Complete the minimum configuration for a manually configured IPsec SA.

**Example**

```

Hostname(config)# crypto map mymap 3 ipsec-manual
Hostname(config-crypto-map)# set peer 2.2.2.2
Hostname(config-crypto-map)# set session-key inbound esp 301 cipher
abcdef1234567890
Hostname(config-crypto-map)# set session-key outbound esp 300 cipher
abcdef1234567890
Hostname(config-crypto-map)# set transform-set myset
Hostname(config-crypto-map)# match address 101

```

#Complete the minimum configuration for an IPsec SA negotiated via IKE.

```

Hostname(config)# crypto map mymap 4 ipsec-isakmp
Hostname(config-crypto-map)# set peer 2.2.2.2
Hostname(config-crypto-map)# set transform-set myset
Hostname(config-crypto-map)# match address 101

```

**Verification** N/A

## 15.30 crypto map (interface IPsec)

Use this command to apply a defined encryption mapping set to an interface.

**crypto map** *map-name*

Use the **no** form of this command to cancel the association between an interface and an encryption mapping set.

**no crypto map** [*map-name*]

| Parameter Description | Parameter       | Description                                      |
|-----------------------|-----------------|--------------------------------------------------|
|                       | <i>map-name</i> | Indicates the name of an encryption mapping set. |

**Defaults** No encryption mapping set is applied to an interface by default.

**Command Mode** Interface configuration mode

**Default Level** 14



**Usage Guide** Use this command to apply an encryption mapping set to an interface. An encryption mapping set must be applied to an interface so that IPsec encryption and protection can be provided for data on the interface. One interface can be associated with only one encryption mapping set. If multiple encryption mapping entries share the same **map-name** value but have different **seq-num** values, these encryption mapping entries belong to the same encryption mapping set and are applied to the same interface. The encryption mapping entry with a smaller **seq-num** value has a higher priority and is used for data matching first. One encryption mapping set can be configured only on one interface.

**Configuration** #Apply the encryption mapping set named mymap to Interface s0.

**Example**

```

Hostname(config)# interface serial 0
Hostname(config-if-Serial 0)# crypto map mymap

```

**Verification** N/A

## 15.31 crypto map local-address

Use this command to specify the IPsec local address.

**crypto map** *map-name* **local-address** *interface-type* *interface-number*

Use the **no** form of this command to cancel the specified IPsec local address.

**no crypto map** *map-name* **local-address**

| Parameter Description | Parameter               | Description                                                                                           |
|-----------------------|-------------------------|-------------------------------------------------------------------------------------------------------|
|                       | <i>map-name</i>         | Indicates the name of an IPsec encryption mapping set.                                                |
|                       | <i>interface-type</i>   | Indicates the type of the interface of which the address is used as the IPsec local address.          |
|                       | <i>interface-number</i> | Indicates the serial number of the interface of which the address is used as the IPsec local address. |

**Defaults** The address of the outbound interface of IPsec data is used as the IPsec local address by default.

**Command** Global configuration mode

**Mode**

**Default Level** 14

**Usage Guide** If an encryption mapping set is applied to multiple interfaces and this command is not executed, the device running RGOS creates an IPsec SA for each interface with the same remote peer and the same ACL. The IP address of the interface that sends and receives encryption traffic is used as the local address by default. After this command is executed to specify the local address, if the same encryption mapping set is applied to multiple interfaces, only one IPsec SA is created for communication. If multiple interfaces on one device support IPsec communication, use this command to specify the IPsec local address to facilitate management. In this way, the device running RGOS uses a fixed address to

communicate with external routers.

In general, it is recommended to use the IP address of the loopback interface as the IPsec local interface.

**Configuration** #Specify the address of the Loopback0 interface as the IPsec local address.

**Example** `Hostname(config)# crypto map mymap local-address loopback 0`

**Verification** N/A

## 15.32 crypto mib enable

Use this command to enable IPsec MIB.

**crypto mib enable**

Use the **no** form of this command to restore the default settings.

**no crypto mib enable**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       |             |

**Defaults** The IPsec MIB is disabled by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** The MIB management involves the statistics of data flow and data packet encryption, which may affect the IPsec data communication. Therefore, IPsec MIB statistics is disabled by default. To visit MIB, run this command.

**Configuration** The following example enables IPsec MIB.

**Example** `Hostname(config)# crypto mib enable`

## 15.33 encryption (IKE policy)

Use this command to specify the encryption algorithm for IKE policies.

**encryption { des | 3des | aes-128 | aes-192 | aes-256 }**

Use the **no** form of this command to restore the default encryption algorithm.

**no encryption**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                              |                                                                                                                                                            |                                                                     |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Description</b>           |                                                                                                                                                            |                                                                     |
|                              | <b>des</b>                                                                                                                                                 | Specifies the 56-bit DES-CBC as the encryption algorithm.           |
|                              | <b>3des</b>                                                                                                                                                | Specifies the 168-bit DES-CBC as the encryption algorithm.          |
|                              | <b>aes-128</b>                                                                                                                                             | Specifies the AES with the 128-bit key as the encryption algorithm. |
|                              | <b>aes-192</b>                                                                                                                                             | Specifies the AES with the 192-bit key as the encryption algorithm. |
|                              | <b>aes-256</b>                                                                                                                                             | Specifies the AES with the 256-bit key as the encryption algorithm. |
| <b>Defaults</b>              | The 56-bit DES-CBC encryption algorithm is used by default.                                                                                                |                                                                     |
| <b>Command Mode</b>          | IKE policy configuration mode                                                                                                                              |                                                                     |
| <b>Default Level</b>         | 14                                                                                                                                                         |                                                                     |
| <b>Usage Guide</b>           | The data encryption algorithm specified by this command is used for encryption of IKE SA data. It differs from the encryption algorithm used by IPsec SAs. |                                                                     |
| <b>Configuration Example</b> | #Specify DES as the encryption algorithm for IKE policies.                                                                                                 |                                                                     |
| <b>Example</b>               | <pre> Hostname(config)# crypto isakmp policy 10 Hostname(isakmp-policy)# encryption des </pre>                                                             |                                                                     |
| <b>Verification</b>          | N/A                                                                                                                                                        |                                                                     |

## 15.34 group (IKE policy)

Use this command to specify the ID of the Diffie-Hellman group in IKE policies.

**group { 1 | 2 | 5 }**

Use the **no** form of this command to restore the default ID of the Diffie-Hellman group.

**no group**

| <b>Parameter Description</b> |           |                                              |
|------------------------------|-----------|----------------------------------------------|
|                              | Parameter | Description                                  |
|                              | <b>1</b>  | Indicates the 768-bit Diffie-Hellman group.  |
|                              | <b>2</b>  | Indicates the 1024-bit Diffie-Hellman group. |
|                              | <b>5</b>  | Indicates the 1536-bit Diffie-Hellman group. |

**Defaults** The 768-bit Diffie-Hellman group (group 1) is used by default.

**Command Mode** IKE policy configuration mode

**Default Level** 14

**Usage Guide** Use this command to specify the Diffie-Hellman group to be used in an IKE policy.

**Configuration** #Specify the 1024-bit Diffie-Hellman group for an IKE policy.

**Example**

```

Hostname(config)# crypto isakmp policy 10
Hostname(isakmp-policy)# group 2

```

**Verification** N/A

**Platform Description** Group 5 is supported in the 11.1PJ33 project for the first time.

## 15.35 hash (IKE policy)

Use this command to specify the hash algorithm for IKE policies.

**hash { sha | md5 }**

Use the **no** form of this command to restore the default hash algorithm.

**no hash**

| Parameter Description | Parameter  | Description                                           |
|-----------------------|------------|-------------------------------------------------------|
|                       | <b>sha</b> | Specifies SHA-1 (HMAC variant) as the hash algorithm. |
|                       | <b>md5</b> | Specifies MD5 (HMAC variant) as the hash algorithm.   |
|                       | <b>sm3</b> | Specifies SM3 as the hash algorithm.                  |

**Defaults** SHA is used as the hash algorithm by default.

**Command Mode** IKE policy configuration mode

**Default Level** 14

**Usage Guide** Use this command to specify the hash algorithm to be used in an IKE policy.

**Configuration** #Specify MD5 as the hash algorithm.

**Example**

```

Hostname(config)# crypto isakmp policy 10
Hostname(isakmp-policy)# hash md5

```

**Verification** N/A

## 15.36 lifetime (IKE policy)

Use this command to specify the lifetime of IKE SAs.

**lifetime** *seconds*

Use the **no** form of this command to restore the default IKE SA lifetime.

**no lifetime**

| Parameter Description | Parameter      | Description                                                                                       |
|-----------------------|----------------|---------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Indicates the IKE SA lifetime in seconds. The value is an integer in the range from 60 to 86,400. |

**Defaults** The default value is 86,400 seconds (1 day).

**Command Mode** IKE policy configuration mode

**Default Level** 14

**Usage Guide** Use this command to specify the lifetime of IKE SAs. When starting negotiation, IKE first reaches an agreement on session security parameters with the peer IKE. These consistent parameters will be referenced by IKE SAs on each peer and are retained on each peer till the IKE SA lifetime times out. A new SA must be negotiated prior to the expiration of the current SA. IPsec SAs are negotiated on the basis of IKE SAs. Therefore, a longer lifetime should be configured for IKE SAs to shorten the time required for negotiating IPsec SAs. However, the cracking probability is directly proportional to the lifetime. A longer lifetime indicates a higher cracking probability while a shorter lifetime indicates a lower cracking probability. Therefore, set a proper lifetime (for example, 43,200 seconds) as required.

**Configuration** #Set the IKE SA lifetime to 1,000 seconds.

**Example**

```

Hostname(config)# crypto isakmp policy 10
Hostname(isakmp-policy)# lifetime 1000

```

**Verification** N/A

## 15.37 match address (IPSec)

Use this command to specify an ACL for an encryption mapping entry.

**match address** *access-list-number*

Use the **no** form of this command to delete an ACL from an encryption mapping entry.

**no match address**

| Parameter Description        | Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Description                                                                                                      |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
|                              | <i>access-list-number</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Indicates the ACL No. (100-199, 2000-2699, and 2900-3899). Encryption mapping entries use only IP extended ACLs. |
| <b>Defaults</b>              | No ACL is specified in encryption mapping entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                  |
| <b>Command Mode</b>          | Encryption mapping configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                  |
| <b>Default Level</b>         | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                  |
| <b>Usage Guide</b>           | <p>Use this command to specify an ACL for an encryption mapping entry. The device determines whether data needs to be protected through IPsec according to the ACL in encryption mapping entry.</p> <p>The ACL specified by this command is applied to both outbound and inbound communication. If it is detected that outbound data matches the ACL and an SA is already established, the device encrypts and forwards the data. If no SA is established, the device triggers the SA negotiation (using IKE). If it is detected that inbound data matches the ACL, the device decrypts the encrypted data and directly discards data that is not encrypted.</p> |                                                                                                                  |
| <b>Configuration Example</b> | <p>#Associate ACL 101 with the encryption mapping set named <b>mymap</b>.</p> <pre> Hostname(config)# crypto map mymap 4 ipsec-isakmp Hostname(config-crypto-map)# match address 101 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                  |
| <b>Verification</b>          | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                  |

## 15.38 match any

Use this command to configure the local and remote IP addresses and masks as 0.0.0.0/0.0.0.0 for specified flows.

**match any**

Use the **no** form of this command to cancel the configuration.

**no match any**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | -         | -           |

**Defaults** The local and remote IP addresses and masks are not set to 0.0.0.0/0.0.0.0 for specified flows by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** This command is used to configure local and remote IP addresses and masks as 0.0.0.0/0.0.0.0 for specified flows in a profile. The profile is mainly used for IPsec over GRE and L2TP over IPsec.  
If this command is configured for IPsec over GRE, local and remote IP addresses and masks of specified flows are 0.0.0.0/0.0.0.0 in phase 2 negotiation.

**Configuration Example** The following example configures local and remote IP addresses and masks as 0.0.0.0/0.0.0.0 for specified flows in the profile named **test**.

```
Hostname(config)# crypto ipsec profile test
Hostname(config-crypto-profile)# match any
```

**Verification** -

**Notifications** -

**Common Errors** -

**Platform Description** -

## 15.39 mode (IPsec)

Use this command to configure the encapsulation mode of transform sets.

**mode { transport | tunnel }**

Use the **no** form of this command to restore the default mode.

**no mode**

| Parameter Description | Parameter        | Description                                                      |
|-----------------------|------------------|------------------------------------------------------------------|
|                       | <b>transport</b> | Sets the encapsulation mode of transform sets to transport mode. |
|                       | <b>tunnel</b>    | Sets the encapsulation mode of transform sets to tunnel mode.    |

**Defaults** The tunnel mode is used by default.

**Command Mode** Transform set configuration mode

**Default Level** 14

**Usage Guide** The configured mode takes effect for only communication using addresses of IPsec peers as the source and

destination addresses. Other communication is performed in tunnel mode.

If the source and destination addresses of the communication to be protected are those of IPsec peers and the transport mode is specified, the device requests the transport mode during negotiation but accepts both the transport mode and tunnel mode. If the tunnel mode is specified, the device requests the tunnel mode and accepts only the tunnel mode.

**Configuration Example** The following example configures the encapsulation mode of transform sets as tunnel mode.

```

Hostname(config)# crypto ipsec transform-set myset ah-md5-hmac
Hostname(cfg-crypto-trans)# mode tunnel
Hostname(cfg-crypto-trans)# mode transport

```

**Verification** -

**Notifications** -

**Common** -

**Errors**

**Platform** -

**Description**

## 15.40 reverse-route

Use this command to enable the reverse route injection function. When this command is configured, the IPsec module automatically adds a static route destined for the peer end of a tunnel or a specified IP address after the negotiation of the tunnel is completed.

**reverse-route** [ **no-peer** | **remote-peer** *ip-address* ] [ *distance* ]

Use the **no** form of this command to disable the reverse route injection function.

**no reverse-route**

| Parameter Description | Parameter                            | Description                                                        |
|-----------------------|--------------------------------------|--------------------------------------------------------------------|
|                       | <b>no-peer</b>                       | Indicates that the next-hop address is not specified.              |
|                       | <b>remote-peer</b> <i>ip-address</i> | (Optional) Specifies the next-hop address.                         |
|                       | <i>distance</i>                      | Specifies the next-hop distance. The value range is from 1 to 255. |

**Defaults** The reverse route injection function is disabled by default.

**Command Mode** Encryption mapping configuration mode



**Default Level** 14

**Usage Guide** no-peer is used to directly destine the route to the interface without specifying the next-hop for PPPoE etc. You can run the **show ip route** command to display added routes. You can run the **debug crypto ipsec** command to display information about added routes and deleted routes.

**Configuration** #Enable the reverse route injection function in the mapping encryption entry named mymap.

**Example**

```

Hostname(config)# crypto map mymap 5 ipsec-isakmp
Hostname(config-crypto-map)# reverse-route

```

**Verification** N/A

## 15.41 self-identity

Use this command to specify the form of the local identity.

**self-identity** { **address** | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }

Use the **no** form of this command to restore the default local identity form.

**no self-identity**

| Parameter Description | Parameter        | Description                                   |
|-----------------------|------------------|-----------------------------------------------|
|                       | <b>address</b>   | Indicates the local IP address.               |
|                       | <i>fqdn</i>      | Indicates the local domain name.              |
|                       | <i>user-fqdn</i> | Indicates the local username and domain name. |

**Defaults** The local identity uses the local IP address by default.

**Command Mode** Global configuration mode

**Default Level** 14

**Usage Guide** Use this command to set the identity for the negotiation initiated in aggressive mode. You can use the domain name or address to specify the local identity.

**Configuration** #Set the local identity.

**Example**

```

Hostname(config)# self-identity fqdn www.vpdn.com
Hostname(config)# self-identity address

```

**Verification** N/A

## 15.42 set autoup

Use this command to set tunnel auto-connection.

**set autoup**

Use the **no** form of this command to restore the default configuration.

**no set autoup**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | -         | -           |

**Defaults** Tunnel auto-connection is disabled by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** Use this command to prevent packet loss caused by tunnel negotiation. Use this function in scenarios where data transmission is sensitive to tunnels and the tunnels need to be in the Up state at any time.

**Configuration** #Set the tunnel auto-connection.

**Example**

```

Hostname(config)# crypto map mymap 10 IPsec-isakmp
Hostname(config-crypto-map)# set autoup

```

**Verification** N/A

## 15.43 set exchange-mode

Use this command to set the work mode used in Phase 1 of IKE negotiation between peers.

**set exchange-mode { main | aggressive }**

Use the **no** form of this command to restore the default work mode.

**no set exchange-mode**

| Parameter Description | Parameter         | Description                    |
|-----------------------|-------------------|--------------------------------|
|                       | <b>main</b>       | Indicates the main mode.       |
|                       | <b>aggressive</b> | Indicates the aggressive mode. |

**Defaults** The main mode is used by default.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Command Mode</b>  | Encryption mapping configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Default Level</b> | 14                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Usage Guide</b>   | <p>The IKE negotiation includes two phases:</p> <p>In Phase 1, a secure channel that passes authentication is established between two ISAKMP entities. The main mode or aggressive mode can be adopted in this phase.</p> <p>In Phase 2, service SAs are negotiated.</p> <p>Select the required work mode in Phase 1 based on their advantages and disadvantages. The main mode is adopted by default. When IP addresses are not statically configured, the aggressive mode is recommended.</p> |
| <b>Configuration</b> | #Set the work mode to aggressive mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Example</b>       | <pre> Hostname(config)# crypto map mymap 10 IPsec-isakmp Hostname(config-crypto-map)# <b>set exchange-mode aggressive</b> </pre>                                                                                                                                                                                                                                                                                                                                                                |
| <b>Verification</b>  | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 15.44 set isakmp-policy

Use this command to specify a policy for negotiating a mapping set.

**set isakmp-policy** *number*

Use the **no** form of this command to cancel a policy for negotiation.

**no set isakmp-policy**

| Parameter Description | Parameter     | Description                                                          |
|-----------------------|---------------|----------------------------------------------------------------------|
|                       | <i>number</i> | Indicates the serial number of the specified policy for negotiation. |

**Defaults** No policy is specified for negotiation by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** In aggressive mode, the device in the branch sends the policy of the highest priority to the device in the headquarters for negotiation by default. Therefore, if the same device in the branch negotiates with multiple devices in the headquarters in aggressive mode, the policy of the highest priority on each device in the headquarters needs to be consistent with that on the device in the branch, which reduces device compatibility. Use this command to specify a policy for negotiating a mapping set. In this way, the policy of the highest priority on each device in the headquarters does not need to be consistent with that on the

device in the branch. This command is effective only to static mapping sets and is unavailable to dynamic mapping sets.

**Configuration** #Specify the policy with the serial number 2 for negotiation in the static mapping set named xyz.

**Example**

```
11.x_sitel(config)#crypto map xyz 100 ipsec-isakmp
11.x_sitel(config-crypto-map)#set isakmp-policy 2
```

**Verification** N/A

## 15.45 set local (IPSec)

Use this command to specify the local IP address in an encryption mapping entry.

**set local** *ip-address*

Use the **no** form of this command to delete the local peer from an encryption mapping entry.

**no set local** *ip-address*

| Parameter Description | Parameter         | Description                     |
|-----------------------|-------------------|---------------------------------|
|                       | <i>ip-address</i> | Indicates the local IP address. |

**Defaults** No local peer is specified by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** Use this command to set the local IP address used in the negotiation. The main address of the interface is used for negotiation when the IP address is not configured. The specified IP address is used for negotiation after configuration.

**Configuration** #Specify a local IP address (2.2.2.3) in the mapping encryption entry named mymap.

**Example**

```
Hostname(config)# crypto map mymap 5 IPSec-isakmp
Hostname(config-crypto-map)# set local 2.2.2.2
```

**Verification** N/A

## 15.46 set mtu

Use this command to set the IPSec pre-fragmentation mode (valid in tunnel mode).

**set mtu** *length*

Use the **no** form of this command to disable the IPsec pre-fragmentation mode.

**no set mtu**

| Parameter Description | Parameter     | Description                                                                                                |
|-----------------------|---------------|------------------------------------------------------------------------------------------------------------|
|                       | <i>length</i> | Indicates the size of a data packet fragment prior to encapsulation. The value range is from 512 to 1,500. |

**Defaults** The IPsec pre-fragmentation mode is disabled by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** Specify the pre-fragmentation mode for IPsec tunnel encapsulation.

**Configuration** #Specify the pre-fragmentation mode in the encryption mapping set named mymap.

**Example**

```

Hostname(config)# crypto map mymap 5 IPsec-isakmp
Hostname(config-crypto-map)# set mtu 1000

```

**Verification** N/A

## 15.47 set peer (IPsec)

Use this command to specify a remote peer in an encryption mapping entry.

**set peer** { *hostname* | *ip-address* }

Use the **no** form of this command to delete the remote peer from an encryption mapping entry.

**no set peer** { *hostname* | *ip-address* }

| Parameter Description | Parameter         | Description                                  |
|-----------------------|-------------------|----------------------------------------------|
|                       | <i>ip-address</i> | Indicates the IP address of the remote peer. |
|                       | <i>hostname</i>   | Indicates the host name of the remote peer.  |

**Defaults** No remote peer is specified by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** A remote peer must be specified for an encryption mapping entry in use.

When there are multiple certificate chains locally, specify the certificate chain according to each peer. If no local certificate chain is specified, the peer certificate chain (CA certificate) is used for authentication. When the peer certificate chain is not specified, the default certificate chain (CA certificate) is used for authentication.

**Configuration** #Specify a remote peer (2.2.2.2) in the mapping encryption entry named mymap.

**Example**

```
Hostname(config)# crypto map mymap 5 ipsec-isakmp
Hostname(config-crypto-map)# set peer 2.2.2.2
```

**Verification** N/A

## 15.48 set peer-identical

Use this command to specify multiple ACEs to use the same remote peer in the negotiation in Phase 2.

**set peer-identical**

Use the **no** form of this command to delete the same remote peer configured in multiple ACEs used in the negotiation in Phase 2.

**no set peer-identical**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** No identical remote peer is specified for multiple ACEs in the negotiation in Phase 2 by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** When multiple ACEs are configured in an ACL and multiple remote peers are configured, use this command to ensure that all ACEs use the same peer for negotiation.

**Configuration** #Specify ACEs to use the same remote peer in the encryption mapping entry named mymap.

**Example**

```
Hostname(config)# crypto map mymap 5 ipsec-isakmp
Hostname(config-crypto-map)# set peer-identical
```

**Verification** N/A

## 15.49 set peer-preempt

Use this command to specify the remote peer of a higher priority to initiate preemption.

**set peer-preempt**

Use the **no** form of this command cancel the configuration of requesting the remote peer of a higher priority to initiate preemption.

**no set peer-preempt**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** No remote peer of a higher priority is specified to initiate preemption by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** Use the peer of a higher priority for negotiation when multiple remote peers are configured. Multiple remote peers can be configured for one encryption mapping set. A remote peer configured earlier has a priority higher than that of a remote peer configured later. The peer of a higher priority is used for negotiation. When the device switches to another peer for negotiation after a tunnel is interrupted, if the peer of a higher priority can initiate negotiation, the peer of the higher priority is used for negotiation and forwarding and the tunnel negotiation using the peer of a lower priority is interrupted. This command must be configured to implement the preceding functions.

**Configuration Example** #Specify the remote peer of a higher priority to initiate preemption in the encryption mapping set named mymap.

```
Hostname(config)# crypto map mymap 5 IPsec-isakmp
Hostname(config-crypto-map)# set peer-preempt
```

**Verification** N/A

## 15.50 set pfs (IPSec)

Use this command to specify the Diffie-Hellman group ID used in IPsec tunnel encapsulation.

**set pfs { group1 | group2 }**

Use the **no** form of this command to cancel the Diffie-Hellman group ID used in tunnel encapsulation.

**no set pfs**

| Parameter Description | Parameter | Description                   |
|-----------------------|-----------|-------------------------------|
|                       | group1    | Indicates the 768-bit group.  |
|                       | group2    | Indicates the 1024-bit group. |

|               |                               |
|---------------|-------------------------------|
| <b>group5</b> | Indicates the 1536-bit group. |
|---------------|-------------------------------|

**Defaults** No Diffie-Hellman group is used by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** Specify the Diffie-Hellman group ID used in IPsec tunnel encapsulation.

**Configuration** #Specify the 1024-bit Diffie-Hellman group in the encryption mapping set named mymap.

**Example**

```

Hostname(config)# crypto map mymap 5 IPsec-isakmp
Hostname(config-crypto-map)# set pfs group2

```

**Verification** N/A

## 15.51 set security-association lifetime

Use this command to set the global lifetime used for IPsec SA association in an encryption mapping set.

**set security-association lifetime { seconds *seconds* | kilobytes *kilobytes* }**

Use the **no** form of this command to restore the default value of global lifetime used for IPsec SA association in an encryption mapping set.

**no set security-association lifetime { seconds | kilobytes }**

| Parameter Description | Parameter                         | Description                                                                                                     |
|-----------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------|
|                       | <b>seconds</b> <i>seconds</i>     | Indicates the SA timeout period in seconds. The value range is from 120 to 86400.                               |
|                       | <b>kilobytes</b> <i>kilobytes</i> | Indicates the timeout communication amount of an SA in kilobytes. The value range is from 2,560 to 536,870,912. |

**Defaults** SAs in an encryption mapping set are negotiated based on the global lifetime.


**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** This command is effective only to encryption mapping entries used for negotiation of IPsec SAs established via IKE and is unavailable to encryption mapping entries of SAs that are manually configured. By default, all IPsec SAs are negotiated based on the global lifetime. If a different lifetime is required for SA negotiation for a specific destination IP address, use this command to change the lifetime in the



encryption mapping entry that uses this destination address for negotiation.

 This command changes the lifetime for IPsec SA negotiation in a specific encryption entry and does not affect the global lifetime.

**Configuration** #Change the lifetime of Entry 5 to 2,500 seconds in the encryption mapping set named mymap.

**Example**

```
Hostname(config)# crypto map mymap 5 IPsec-isakmp
Hostname(config-crypto-map)# set security-association lifetime seconds 2500
```

**Verification** N/A

## 15.52 set session-key

Use this command to configure the security parameter index (SPI) and password of a specified algorithm for inbound and outbound protected communication.

**set session-key** { inbound | outbound } ah *spi hex-key-data*

**set session-key** { inbound | outbound } esp *spi* { authenticator *hex-key-data* | cipher *hex-key-data* }

Use the **no** form of this command to delete the SPI and password of a specified algorithm.

**no set session-key** { inbound | outbound } ah

**no set session-key** { inbound | outbound } esp

| Parameter Description | Parameter           | Description                    |
|-----------------------|---------------------|--------------------------------|
|                       | <i>spi</i>          | Specifies the SPI.             |
|                       | <i>hex-key-data</i> | Indicates the hexadecimal key. |

**Defaults** The SPI and password of a specified algorithm are not specified.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** This command is used for manually created SAs.

**Configuration Example** The following example specifies ESP encryption and decryption password of abcdef1234567890 in the crypto map named **mymap**.

```
Hostname(config)# crypto map mymap 5 ipsec-manual
Hostname(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
Hostname(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
```

**Verification** -

|               |   |
|---------------|---|
| Notifications | - |
| Common        | - |
| Errors        | - |
| Platform      | - |
| Description   | - |

## 15.53 set transform-set

Use this command to specify transformation sets to be used in an encryption mapping entry.

**Set transform-set** *transform-set-name1* [ *transform-set-name2* ] [ *transform-set-name3* ] [ *transform-set-name4* ] [ *transform-set-name5* ] [ *transform-set-name6* ]

Use the **no** form of this command to delete all transformation sets from an encryption mapping entry.

**no set pfs**

| Parameter Description | Parameter                                                                                                                                                                                                  | Description                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>transform-set-name1</i> ,<br>[ <i>transform-set-name2</i> ],<br>[ <i>transform-set-name3</i> ],<br>[ <i>transform-set-name4</i> ],<br>[ <i>transform-set-name5</i> ],<br>[ <i>transform-set-name6</i> ] | Indicates the name of a transformation set. A maximum of six transformation sets can be specified in one encryption mapping entry. |

**Defaults** No transformation set is specified by default.

**Command Mode** Encryption mapping configuration mode

**Default Level** 14

**Usage Guide** A transformation set is indispensable for successful establishment of an SA. Use this command to specify a transformation set when any encryption mapping set is configured.

**Configuration** #Specify the transformation set named myset in the encryption mapping entry.

**Example**

```

Hostname(config)# crypto IPsec transform-set myset esp-des esp-sha-hmac
Hostname(config)# crypto map mymap 5 IPsec-isakmp
Hostname(config-crypto-map)# set transform-set myset

```

**Verification** N/A

## 15.54 show crypto dynamic-map (IPSec)

Use this command to display dynamic encryption mapping information.

**show crypto dynamic-map** [ *map-name* ]

| Parameter Description | Parameter       | Description                                      |
|-----------------------|-----------------|--------------------------------------------------|
|                       | <i>map-name</i> | Indicates the name of an encryption mapping set. |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** Use this command to display the PIM interfaces on the device, PIM neighbors of interfaces, Hello message retransmission interval, DR address, and other information.

**Configuration** #Display information about all dynamic encryption mapping sets.

**Example**

```

Hostname# show crypto dynamic-map
      Crypto Map Template "mydmap" 1
No matching address list set.
Security association lifetime: 4608000 kilobytes/3600 seconds(id=34)
PFS (Y/N): N
Transform sets = { }
```

## 15.55 show crypto ipsec sa

Use this command to display information about the current active IPsec SA.

**show crypto ipsec sa**

| Parameter Description | Parameter                                                          | Description                              |
|-----------------------|--------------------------------------------------------------------|------------------------------------------|
|                       | <b>interface</b> <i>interface-type</i><br><i>interface-number-</i> | Specifies the interface type and number. |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration** #Display information about the current active IPsec SA.

**Example**

```

Hostname# show crypto ipsec sa
Interface: GigabitEthernet 0/1
    Crypto map tag:mymap, local addr 2.2.2.3
    media mtu 1500
    sub_map type:static, seqno:7, id=0
    local ident (addr/mask/prot/port): (2.2.2.3/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (2.2.2.2/0.0.0.0/0/0)
    PERMIT
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #send errors 0, #recv errors 0
    Inbound esp sas:
        spi:0x79b8e4bb (2042160315)
        transform: esp-3des
        in use settings={Tunnel,}
        crypto map mymap 7
        sa timing: remaining key lifetime (k/sec): (4607000/3505)
        IV size: 8 bytes
        max reply windows size: 0
        Replay detection support:Y

    Outbound esp sas:
        spi:0x293b8b55 (691768149)
        transform: esp-3des
        in use settings={Tunnel,}
        crypto map mymap 7
        sa timing: remaining key lifetime (k/sec): (4607000/3505)
        IV size: 8 bytes
        max reply windows size: 0
        Replay detection support:Y

```

## 15.56 show crypto ipsec transform-set

Use this command to display information about transformation sets configured for the device.

**show crypto ipsec transform-set**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration** #Display information about transformation sets configured for the device.

**Example**

```

Hostname# show crypto ipsec transform-set
transform set myset3: { esp-des, }
will negotiate = {Tunnel, }

```

## 15.57 show crypto isakmp policy

Use this command to display the IKE policy configured for the device.

**show crypto isakmp policy**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Command Mode** Privileged EXEC mode

**Default Level** 14

**Usage Guide** N/A

**Configuration** #Display the IKE policy configured for the device.

**Example**

```

Hostname# show crypto isakmp policy
Protection suite of priority 9
encryption algorithm: 3DES - Data Encryption Standard (56 bit keys).
hash algorithm:      Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime:           1000 seconds
Protection suite of priority 10
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm:      Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime:           1000 seconds
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm:      Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)

```

```
lifetime: 86400seconds
```

## 15.58 map (IPSec)

Use this command to display information about an encryption mapping set.

**show crypto map** [ *map-name* ]

| Parameter Description        | Parameter                                                                                                                                                                                                                                                                                       | Description                                      |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
|                              | <i>map-name</i>                                                                                                                                                                                                                                                                                 | Indicates the name of an encryption mapping set. |
| <b>Command Mode</b>          | Privileged EXEC mode                                                                                                                                                                                                                                                                            |                                                  |
| <b>Default Level</b>         | 14                                                                                                                                                                                                                                                                                              |                                                  |
| <b>Usage Guide</b>           | N/A                                                                                                                                                                                                                                                                                             |                                                  |
| <b>Configuration Example</b> | Display information about all encryption mapping sets.                                                                                                                                                                                                                                          |                                                  |
|                              | <pre> Hostname# show crypto map  Crypto Map:"mymap1" 1 ipsec-isakmp, (Complete)   Extended IP access list 100   Security association lifetime: 0 kilobytes/120 seconds(id=2)   PFS (Y/N): N   Transform sets = { myset3,  }  Interfaces using crypto map mymap1:   GigabitEthernet 1/1/0 </pre> |                                                  |
| <b>Notifications</b>         | -                                                                                                                                                                                                                                                                                               |                                                  |
| <b>Platform Description</b>  | -                                                                                                                                                                                                                                                                                               |                                                  |

# 1 PPPoE Client Commands

## 1.1 clear dialer

Use this command to clear statistics about the DDR dialer interface.

**clear dialer**

| <b>Parameter Description</b>  | Parameter                                                               | Description |
|-------------------------------|-------------------------------------------------------------------------|-------------|
|                               | N/A                                                                     | N/A         |
| <b>Command Modes</b>          | Global configuration mode                                               |             |
| <b>Usage Guide</b>            | N/A                                                                     |             |
| <b>Configuration Examples</b> | The following example clears statistics about the DDR dialer interface. |             |
|                               | <pre>R1# clear dialer</pre>                                             |             |
| <b>Platform Description</b>   | N/A                                                                     |             |

## 1.2 clear pppoe tunnel

Use this command to clear all PPPoE tunnels.

**clear pppoe tunnel**

| <b>Parameter Description</b>  | Parameter                                       | Description |
|-------------------------------|-------------------------------------------------|-------------|
|                               | N/A                                             | N/A         |
| <b>Command Modes</b>          | Privileged EXEC mode                            |             |
| <b>Usage Guide</b>            | N/A                                             |             |
| <b>Configuration Examples</b> | The following example clears all PPPoE tunnels. |             |
|                               | <pre>R1# clear pppoe tunnel</pre>               |             |
| <b>Platform Description</b>   | N/A                                             |             |

## 1.3 dialer pool

Use this command to associate a dialer pool with a logical interface.

**dialer pool** *number*

Use the **no** form of this command to restore the default setting.

**no dialer pool** *number*

### Parameter Description

| Parameter     | Description                                               |
|---------------|-----------------------------------------------------------|
| <i>number</i> | Sets the ID of a dialer pool, in the range from 1 to 255. |

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

### Modes

**Usage Guide** Advanced dialup requires association between a physical interface and a dialer interface through a dialer pool. First, add a physical interface to several dialer pools. Second, associate the logical interface with only one of the dialer pools. One physical interface may belong to multiple dialer pools but one logical interface is allowed to associate with one single dialer pool. The dialer interface selects an idle physical interface from the dialer pool randomly.

**Configuration** The following example associates dialer pool 1 with dialer interface1.

### Examples

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer pool 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer pool
```

**Platform Description** N/A

## 1.4 dialer-group

Use this command to associate a dialer triggering rule with a DDR dialer interface.

**dialer-group** *group-number*

Use the **no** form of this command to restore the default setting.

**no dialer-group**

### Parameter Description

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|



|                     |                                     |
|---------------------|-------------------------------------|
| <i>group-number</i> | The ID of a dialer triggering rule. |
|---------------------|-------------------------------------|

**Defaults** This function is disabled by default.

**Command** Interface configuration mode

**Modes**

**Usage Guide** The dialer triggering rule is configured by the **dialer-list** command. You should identify what packets can trigger dial before the association.

**Configuration** The following example associates a dialer triggering rule with DDR dialer interface 1.

**Examples**

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer-group 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer-group
```

**Platform**

N/A

**Description**

## 1.5 dialer-list

Use this command to define a dialer triggering rule.

**dialer-list** *dialer-group* **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }

Use the **no** form of this command to restore the default setting.

**no dialer-list** *dialer-group* [ **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* } ]

**Parameter  
Description**

| Parameter                            | Description                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------|
| <i>dialer-group</i>                  | Sets the ID of a dialer triggering rule.                                    |
| <b>protocol</b> <i>protocol-name</i> | Protocol name.                                                              |
| <b>ip</b>                            | Specifies the IP protocol to be used for defining a dialer triggering rule. |
| <b>permit</b>                        | Permits IP packets.                                                         |
| <b>deny</b>                          | Denies IP packets.                                                          |
| <b>list</b>                          | Specifies an access list to be used for defining a dialer triggering rule.  |
| <i>access-list-number</i>            | Sets the ID of an ACL list.                                                 |

**Defaults** This function is disabled by default.

**Command** Global configuration mode

**Modes**

**Usage Guide** This configuration is mandatory to define one or more dialer triggering rules. Use the **dialer-group** command to apply these rules to specific dialer interfaces.

**Configuration** The following example sets dialer triggering rule 1 to **ip**.

**Examples**

```
R1(config)# dialer-list 1 protocol ip permit
```

The following example restores the default setting.

```
R1(config)# no dialer-list 1
```

**Platform**  
**Description** N/A

## 1.6 encapsulation ppp

Use this command to set the encryption protocol to PPP on an interface.

**encapsulation ppp**

Use the **no** form of this command to delete the configured encryption protocol on an interface.

**no encapsulation**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | -         | -           |

**Defaults** The encryption protocol is not configured.

**Command** Interface configuration mode

**Modes**

**Default Level** 14

**Usage Guide** N/A

**Configuration** The following example sets the encryption protocol to PPP on dialer 1.

**Examples**

```
Hostname# configure terminal
Hostname(config)# intrerface dialer 1
Hostname(config-if-dialer 1)# encapsulation ppp
```

**Verification** Run the **show running-config interface dialer 1** command to check whether the configuration exists.

**Notifications** -

**Common Errors**

-

**Platform Description**

-

Use this command to associate a dialer pool with a logical interface.

**dialer pool** *number*

Use the **no** form of this command to restore the default setting.

**no dialer pool** *number*

**Parameter Description**

| Parameter     | Description                                               |
|---------------|-----------------------------------------------------------|
| <i>number</i> | Sets the ID of a dialer pool, in the range from 1 to 255. |

**Defaults**

This function is disabled by default.

**Command**

Interface configuration mode

**Modes****Usage Guide**

Advanced dialup requires association between a physical interface and a dialer interface through a dialer pool. First, add a physical interface to several dialer pools. Second, associate the logical interface with only one of the dialer pools. One physical interface may belong to multiple dialer pools but one logical interface is allowed to associate with one single dialer pool. The dialer interface selects an idle physical interface from the dialer pool randomly.

**Configuration Examples**

The following example associates dialer pool 1 with dialer interface1.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer pool 1
```

The following example restores the default setting.

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer pool
```

**Platform**

N/A

**Description**

## 1.7 ip address

Use this command to enable the IP policy on an interface.

**ip address** { **negotiate** | *ip-address subnet-mask* }

Use this command to disable the IP address acquisition mode.

**no ip address** [ **negotiate** | *ip-address subnet-mask* ]

| Parameter Description         | Parameter                                                                                                                                                                                                                                                          | Description                                                         |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
|                               | <b>negotiate</b>                                                                                                                                                                                                                                                   | Enables an interface to acquire IP address through PPP negotiation. |
|                               | <i>ip-address</i>                                                                                                                                                                                                                                                  | The IP address of a specified interface.                            |
|                               | <i>subnet-mask</i>                                                                                                                                                                                                                                                 | The mask of a specified interface.                                  |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                                                                                |                                                                     |
| <b>Command Modes</b>          | Interface configuration mode                                                                                                                                                                                                                                       |                                                                     |
| <b>Usage Guide</b>            | Use this command to configure the IP policy on a specified dialer interface. If PPP negotiation is enabled, the IP address is distributed by the server. If the IP address is specified manually, it takes effect only after negotiation with the server succeeds. |                                                                     |
| <b>Configuration Examples</b> | The following example sets the IP policy to PPP negotiation.                                                                                                                                                                                                       |                                                                     |
|                               | <pre>R1(config)# interface dialer 1 R1(config-if-dialer 1)# ip address negotiate</pre>                                                                                                                                                                             |                                                                     |
|                               | The following example removes the IP policy configuration.                                                                                                                                                                                                         |                                                                     |
|                               | <pre>R1(config)# interface dialer 1 R1(config-if-dialer 1)# no ip address</pre>                                                                                                                                                                                    |                                                                     |
| <b>Verification</b>           | Run the <b>show running-config interface dialer 1</b> command to check whether the configuration exists. Run the <b>show ip interface brief   includein dialer 1</b> command to check whether the IP address is negotiated and whether the protocol status is Up.  |                                                                     |
| <b>Notifications</b>          | -                                                                                                                                                                                                                                                                  |                                                                     |
| <b>Common Errors</b>          | -                                                                                                                                                                                                                                                                  |                                                                     |
| <b>Platform Description</b>   | -                                                                                                                                                                                                                                                                  |                                                                     |

## 1.8 pppoe enable

Use this command to enable the PPPoE client function on the interface.

**pppoe enable**

Use the **no** form of this command to restore the default setting.

**no pppoe enable**

| Parameter Description         | Parameter                                                                                                                                                                                                                                                                                                                                                                                     | Description |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                               | N/A                                                                                                                                                                                                                                                                                                                                                                                           | N/A         |
| <b>Defaults</b>               | This function is disabled by default.                                                                                                                                                                                                                                                                                                                                                         |             |
| <b>Command</b>                | Interface configuration mode                                                                                                                                                                                                                                                                                                                                                                  |             |
| <b>Modes</b>                  |                                                                                                                                                                                                                                                                                                                                                                                               |             |
| <b>Usage Guide</b>            | This command must be configured on the physical interface or aggregate interface with WAN attributes. If the interface has LAN attributes, this command is not displayed.                                                                                                                                                                                                                     |             |
| <b>Configuration Examples</b> | <p>The following example enables the PPPoE client function on GigabitEthernet 0/1.</p> <pre>R1(config)# interface GigabitEthernet 0/1 R1(config-if- GigabitEthernet 0/1)# pppoe enable</pre> <p>The following example disables the PPPoE client function on GigabitEthernet 0/1.</p> <pre>R1(config)# interface GigabitEthernet 0/1 R1(config-if- GigabitEthernet 0/1)# no pppoe enable</pre> |             |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                                                                                                                                                                                           |             |

## 1.9 pppoe session mac-address

Use this command to configure the MAC address of a PPPoE session.

**pppoe session mac-address *H.H.H***

Use the **no** form of this command to restore the default setting.

**no pppoe session mac-address**

| Parameter Description | Parameter                                                                                                                                                                                                                      | Description                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|                       | <i>H.H.H</i>                                                                                                                                                                                                                   | Specifies the MAC address. |
| <b>Defaults</b>       | This function is disabled by default.                                                                                                                                                                                          |                            |
| <b>Command</b>        | Interface configuration mode                                                                                                                                                                                                   |                            |
| <b>Modes</b>          |                                                                                                                                                                                                                                |                            |
| <b>Usage Guide</b>    | This command can be used to specify the MAC address of the PPPoE session. It can be configured on interfaces, but takes effect on only sub-interfaces. You must enable PPPoE on the interface before configuring this command. |                            |

**Configuration Examples** The following example sets the MAC address of the PPPoE session to 00d0.f822.33f3 on GigabitEthernet 0/1.1.

```
Ruijie (config)# interface GigabitEthernet 0/1
Hostname(config-subif-GigabitEthernet 0/1)#pppoe enable
Hostname(config-subif-GigabitEthernet 0/1)#encapsulation dot1Q 1
Hostname(config-subif-GigabitEthernet 0/1)#pppoe session mac-address
00d0.f822.33f3
```

The following example deletes the MAC address of the PPPoE session on GigabitEthernet 0/1.1.

```
Ruijie (config)# interface GigabitEthernet 0/1
Hostname(config-subif-GigabitEthernet 0/1)#no pppoe session mac-address
```

**Platform** N/A  
**Description**  
**Verification** Run the **show running-config interface gigabitethernet 0/1.1** command to check whether the configuration exists.

**Notifications**  
 PPPoE: must enable PPPoE firstly.

**Common Errors**

**Platform Description**

### 1.10 pppoe-client dial-pool-number

Use this command to add an Ethernet interface to a dialer pool and specifies the dial mode.  
**pppoe-client dial-pool-number** *number* **no-ddr**

Use the **no** form of this command to restore the default setting.  
**no pppoe-client dial-pool-number** *number*

| Parameter Description | Parameter     | Description                   |
|-----------------------|---------------|-------------------------------|
|                       | <i>number</i> | Sets the ID of a dialer pool. |

**Defaults** This function is disabled by default.

**Command Modes** Interface configuration mode

**Usage Guide** Use this command to add an Ethernet interface to a dialer pool, which is associated with the logical interface. In this way, the Ethernet interface and the logical interface are connected to perform dialing. Before configuring this command, enable PPPoE on the interface.

**Configuration** The following example adds GigabitEthernet 0/1 to dialer pool 1.

**Examples**

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if- GigabitEthernet 0/1)# pppoe-client dial-pool-number 1 no-ddr
```

The following example removes GigabitEthernet 0/1 from dialer pool 1.

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if- GigabitEthernet 0/1)# no pppoe-client dial-pool-number 1
```

**Platform**  
**Description** N/A

**Verification** Run the **show running-config interface gGigabiteEthernet 0/15** command to check whether the configuration exists.

**Notifications** PPPoE: must enable PPPoE firstly.

## 1.11 show dialer

Use this command to display DDR dial-up information.

**show dialer [ interface *interface-type interface-number* | maps | pools ]**

| Parameter Description | Parameter                                               | Description                                                |
|-----------------------|---------------------------------------------------------|------------------------------------------------------------|
|                       | <b>interface</b> <i>interface-type interface-number</i> | Displays DDR dial-up information on a specified interface. |
|                       | <b>maps</b>                                             | Displays dial-up mapping information.                      |
|                       | <b>pools</b>                                            | Displays dialer pool information.                          |

**Command** All modes except the user EXEC mode

**Modes**

**Default Level** 14

**Usage Guide** -

**Configuration** -

**Examples** -

**Notifications** -

**Platform****Description**

-

## 1.12 show pppoe

Use this command to display PPPoE information.

**show pppoe { ref | session | tunnel }**

**Parameter  
Description**

| Parameter      | Description                                                    |
|----------------|----------------------------------------------------------------|
| <b>ref</b>     | Displays fast forwarding information about all PPPoE sessions. |
| <b>session</b> | Displays all PPPoE session information.                        |
| <b>tunnel</b>  | Displays all PPPoE tunnel information.                         |

**Command**

Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Modes****Usage Guide** N/A

**Configuration** The following example displays fast forwarding information about all PPPoE sessions.

**Examples**

```
R1# show pppoe ref
```

```
GigabitEthernet 0/6 Virtual-pppoe 2 dialer 1
  Protocol UP dialer-group 1 last_time 164235070 ms
  Ether Header: 00 60 4F 67 02 50 00 D0 F8 22 33 43 88 64
  PPPoE Header: 11 00 00 7F 00 50
  PPP Header   : 00 21
  DstMac 0060.4f67.0250, SrcMAC 00d0.f822.3343, SessionID 127
  Input Err : 0 MAC, 0 PPPoE Header
  Input Info: 0 Normal, 0 Drop, 345 Reserve, 0 Lost
  Output Err : 0 SessionState, 0 no ref, 0 length
  Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost
```

```
There is 1 pppoe session in System
```

The following example displays all PPPoE session information.

```
R1# show pppoe session
```

```
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is
00.60.4F.67.02.50
  Timer is running: 59750
```

The following example displays all PPPoE tunnel information.

```
R1# show pppoe tunnel
```

```
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is
00.60.4F.67.02.50
  Timer is running: 59003
```



|                    |     |
|--------------------|-----|
| <b>Platform</b>    | N/A |
| <b>Description</b> |     |