



XS-S1930J Series Switches

RGOS Command Reference, Release 11.4(1)B70P15

Copyright Statement

Ruijie Networks©2021

Ruijie Networks reserves all copyrights of this document. 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.

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. 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

Thank you for using our products. This manual matches the RGOS Release 11.4(1)B70P15.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- 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
- Skype: [service_rj@ruijienetworks.com](https://www.ruijienetworks.com)

Related Documents

Documents	Description
Configuration Guide	Describes network protocols and related mechanisms that supported by the product, with configuration examples.
Hardware Installation and Reference Guide	Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors.


Conventions


This manual uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[]	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.

Symbols

 Means reader take note. Notes contain helpful suggestions or references.

 Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of

System Configuration Commands

1. Command Line Interface Commands
2. Basic Configuration Management Commands
3. Line Commands
4. File System Commands
5. SYS Commands
6. Time Range Commands
7. HTTP Service Commands
8. Syslog Commands
9. CWMP Commands
10. PoE Management Commands

1 Command Line Interface 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.

```
Ruijie(config)# alias ?
  acl                acl configure mode
  config             globle 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.

```
Ruijie#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:

```
Ruijie#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.

```
Ruijie# 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:

```
Ruijie(config-if)#ia ?
```

```
  A.B.C.D IP address
```

```
  dhcp   IP Address via DHCP
```

```
Ruijie(config-if)# 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.

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:

```
Ruijie# configure terminal
```

```
Ruijie(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

```
Ruijie(config)#def-route?
```

```
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
```

```
Ruijie(config)# end
```

Related Commands N/A

Platform Description N/A

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.
	all	Command alias
	level <i>level</i>	Specifies the execution right levels (0–15) of a command or sub-commands
	reset	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	Description
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:

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

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

```
Ruijie>reload ?
```

```
LINE Reason for reload
```

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

```
Ruijie(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:

```
Ruijie>reload ?
```

```
LINE Reason for reload
```

```
at reload at a specific time/date
```

```
cancel cancel pending reload scheme
```

```
in reload after a time interval
```

```
<cr>
```


**Related
Commands**

Command	Description
enable secret	Sets the CLI-level password.

**Platform
Description**

N/A

2 Basic Configuration Management Commands

2.1 <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 sessions** command to display the session.

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

```
Ruijie# 1
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.2 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 login 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 The following example configures a welcome message.

Examples Ruijie(config)# banner exec \$ Welcome \$

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

2.3 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

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.4 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 Global configuration mode
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.

Configuration The following example configures a login banner.

Examples

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.5 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 Examples The following example configures the MOTD.

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

2.6 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

```
Ruijie(config)# banner prompt-timeout $ authentication timeout $
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.7 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

```
Ruijie(config)# banner slip-ppp $ Welcome $
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.8 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

```
Ruijie# configure
Ruijie(config)#
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.9 disable

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

disable [*privilege-level*]

Parameter Description	Parameter	Description
		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.

```
Ruijie# disable 10
```

Related Commands	Command	Description
		enable

Platform Description N/A

2.10 disconnect

Use this command to disconnect the Telnet Client session.

disconnect *session-id*

Parameter Description	Parameter	Description
		<i>session-id</i>

Defaults N/A

Command Mode User EXEC mode

Usage Guide This command is used to disconnect the Telnet Client session by setting the session ID.

Configuration The following example disconnects the Telnet Client session by setting the session ID.

Examples

```
Ruijie# disconnect 1
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.11 do telnet

Use this command to login to Telnet server.

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

**Parameter
Description**

Parameter	Description
<i>host</i>	IPv4 or host name of Telnet server.
<i>port</i>	Configures TCP port ID. The default is 23, in the range from 0 to 65535.
/source	Specifies source IP or source port for Telnet client.
ip <i>A.B.C.D</i>	Specifies source IPv4 address for Telnet client.
interface <i>interface-name</i>	Specifies source port for Telnet client.

Defaults

N/A

**Command
Mode**

User EXEC mode/Privileged EXEC mode/Interface configuration mode

Usage Guide

N/A

Configuration

The following example telnets to destination IPv6 address 192.168.1.1.

Examples

```
Ruijie(config)# do telnet192.168.1.1 /source interface gigabitEthernet 0/1
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.12 enable

Use this command to enter privileged EXEC mode.

enable [*privilege-level*]

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

Defaults N/A

Command Mode User EXEC mode

Usage Guide Use this command to enter privileged EXEC mode from User EXEC mode. You can raise or lower the privilege level by specifying the privilege level.

Configuration Examples The following example lowers the privilege level to 14:

```
Ruijie> enable 14
Password:
```

Related Commands	Command	Description
		N/A

Platform Description N/A

2.13 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>
	<i>level</i>	User's level.
	0	The password is in plain text.
	7 <i>encrypted-password</i>	The password is encrypted.

Defaults N/A


Command Global configuration mode

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 Ruijie(config)# enable password pw10

Related Commands

Command	Description
enable secret	Sets the security password

Platform

N/A

Description

enable secret Sets the security password

2.14 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 encrypted-secret }

no enable secret [level level]

Parameter Description

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

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.

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

Examples

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

Related Commands	Command	Description
		enable password

Platform Description N/A

2.15 enable service

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

```
enable service { telnet-server | snmp-agent | ssh-server | web-server [ http | https | all ] }
no enable service { telnet-server | snmp-agent | ssh-server | web-server [ http | https | all ] }
```

Parameter Description	Parameter	Description
		ssh-server
	telnet-server	Enables Telnet Server.
	snmp-agent	Enables SNMP Agent.
	web-server [http https all]	Enables Web Server.

Defaults Telnet-server, snmp-agent and web-server are enabled. ssh-server is disabled.

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.

Configuration The following example enables the SSH Server.

Examples

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

Related Commands	Command	Description
		show service

Platform Description N/A

2.16 end

Use this command to return to privileged EXEC mode.

end

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode All modes except privileged EXEC mode

Usage Guide Use this service command to return to privileged EXEC mode.

Configuration Examples The following example returns to privileged EXEC mode.

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

Related Commands	Command	Description
		N/A

Platform Description N/A

2.17 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

Parameter Description	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.

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.18 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

Parameter Description	Parameter	Description
	<i>minutes</i>	Timeout in minutes, in the range from 0 to 35791.
	seconds	(Optional) Timeout in minutes, in the range from 0 to 2147483.

Defaults The default is 10 minutes.

Command Mode Line configuration mode

Usage Guide 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.

Configuration Examples The following example sets the connection timeout to 5'30''.

```
Ruijie(config-line)#exec-timeout 5 30
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.19 execute

Use this command to execute a command on the file.

execute flash: *filename*

Parameter Description	Parameter	Description
	<i>filename</i>	

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

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

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

```
Ruijie#
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

2.20 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 The following example returns to the upper configuration mode.

Examples

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

Press RETURN to get started
```

Related Commands

Command	Description
N/A	N/A

Platform
Description N/A

2.21 help

Use this command to display the help information.

help

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

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

```
Ruijie#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 the parameters of a specified command.

```
Ruijie(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

2.22 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 Mode Global configuration 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 Examples The following example configures the hostname of the device as BeiJingAgenda.

```
Ruijie(config)# hostname BeiJingAgenda
BeiJingAgenda(config)#
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description N/A

2.23 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, including AP port, Gi port, Loopback port, null port, Tunnel port and VLAN port, 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.

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

Related Commands

Command	Description
telnet	Logs in a Telnet server.

Platform Description N/A

2.24 lock

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

lock

Parameter Description

Parameter	Description
N/A	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 The following example locks a terminal interface.

```

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

```

**Related
Commands**

Command	Description
lockable	Supports terminal locking in the line.

Platform

N/A

Description

2.25 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
Mode**

LINE configuration 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. Run the **lockable** command before running the **lock** command.

Configuration

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

```

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

```

```
Password: <password>
```

**Related
Commands**

Command	Description
lock	Locks the terminal.

**Platform
Description**

N/A

2.26 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

Login is disabled for console and enabled for VTY 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

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

**Related
Commands**

Command	Description
password	Configures the line login password

**Platform
Description**

N/A

2.27 login access non-aaa

Use this command to configure non-AAA authentication on line when AAA is enabled. Use the **no** form of this command to restore the default setting.

login access non-aaa

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 N/A

Configuration Examples The following example configures VTY line authentication with AAA enabled.

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.28 login authentication

If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate 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
	default	Name of the default authentication method list

<i>list-name</i>	Name of the method list
------------------	-------------------------

Defaults Default authentication is used when AAA is enabled.

Command Mode Line configuration mode

Usage Guide N/A

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

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

Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
aaa authentication login	Configures the login authentication method list.	

Platform Description N/A

2.29 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

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

Related Commands

Command	Description
username	Configures local user information.

Platform

N/A

Description

2.30 login privilege log

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

login privilege log

no login privilege log

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This command is disabled by default.

Command

Global configuration mode

Mode

Usage Guide

N/A

Configuration

The following example enables the function of logging privilege change.

Examples

```
Ruijie(config)# login privilege log
```

The following example displays the log of privilege change failure.

```
Ruijie>enable 10

Password:
Password:
Password:

% Access denied
Ruijie>

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

The following example displays the log of privilege change success.
```



```
Ruijie>enable 10

Password:
Ruijie#
*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

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

```
Ruijie(config)# line vty 1
Ruijie(config-line)no motd-banner
```

Related Commands	Command	Description

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

Platform
Description N/A

2.32 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>	
0		The password is in plain text.
7 <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 Ruijie(config)# line vty 0
Ruijie(config-line)# password red
```

Related Commands	Command	Description
	login	

Platform
Description N/A

2.33 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
	string	Character string of the prompt 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 The following example sets the prompt string to rgnos.

Examples

```
Ruijie(config)# prompt rgnos
Ruijie(config)# end
rgnos
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.34 secret

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

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


Parameter Description	Parameter	Description
	0	(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 encrypted-secret	Sets the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.

Defaults N/A

Command Line configuration mode

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.

 If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1st, 3rd and 8th characters of the password text must be \$.

In general, the encryption type does not need to be specified as 5 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

```
Ruijie(config)# line vty 0
Ruijie(config-line)# secret vty0
```

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

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

Related Commands	Command	Description
		login

Platform N/A
Description

2.35 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>
	output	Regards data output as the input to determine whether the session expires.

Defaults The default timeout is 0, indicating never timeout.

Command LINE configuration mode
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 Ruijie(config-line)#exec-timeout 5 output

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.36 show debugging

Use this command to display debugging state.

show debugging

**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 debugging state.

Examples Ruijie# show debugging
 acld event debugging is on

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description** N/A

2.37 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
	console	Displays the configuration of a console line, in the range from 0 to 0.
	vty	Displays the configuration of a vty line, in the range from 0 to 35.
	<i>line-num</i>	Number of the line, in the range from 0 to 36.

Defaults N/A

Command Privileged EXEC mode

Mode

Usage Guide N/A

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

Examples

```
Ruijie# 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
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.38 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 N/A

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

Examples

```
Ruijie# show reload
System reload state: Cold
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.39 show running-config

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

show running-config [interface *interface*]

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration N/A

Examples

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.40 show service

Use this command to display the service status.

show service

**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 whether the service is enabled or disabled.

Examples

```
Ruijie# show service
web-server      : disabled
web-server(https) : disabled
snmp-agent      : enabled
ssh-server      : enabled
telnet-server   : disabled
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

2.41 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

```
Ruijie#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

2.42 show startup-config

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

show startup-config

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide The device configuration stored in the NVRAM is executed while the device is starting. On a device that does not support **boot config**, **startup-config** is contained in the default configuration file **/config.text** in the built-in flash memory.

Configuration N/A

Examples

Related Commands	Command	Description
	boot config	Sets the name of the boot configuration file.

Platform Description N/A

2.43 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 Mode Line configuration 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

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.44 telnet

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

telnet *host* [*port*] [/**source** { **ip** *A.B.C.D* | **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, in the range from 0 to 65535.
	/source	Specifies the source IP address or source interface used by the Telnet client.
	ip <i>A.B.C.D</i>	Specifies the source IPv4 address used by the Telnet client.
	interface <i>interface-name</i>	Specifies the source interface used by the Telnet client.

Defaults N/A

Command Mode User EXEC mode

Usage Guide N/A

Configuration Examples N/A

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

Platform Description N/A

2.45 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** { **aux** | **console** | **ssh** | **telnet** }] [**online amount** *number*]

[**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**]
 [**nopassword** | **password** [0 | 7] *text-string*]

no username *name*


Parameter Description

Parameter	Description
<i>name</i>	Username
login mode	Sets the login mode.
aux	Sets the login mode to aux.
console	Sets the login mode to console.
ssh	Sets the login mode to ssh.
telnet	Sets the login mode to telnet.
online amount <i>number</i>	Sets the amount of users online simultaneously, in the range from 0 to 1549. The default is no limit to the number of simultaneous accounts online.
permission <i>oper-mode path</i>	Sets the permission on the specified file. <i>op-mode</i> refers to the operation mode and <i>path</i> to the file or the directory path.
privilege <i>privilege-level</i>	Sets the privilege level, in the range from 0 to 15.
reject remote-login	Confines the account to remote login.
web-auth	Confines the account to web authentication.
nopassword	The account is not configured with a password.
password [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.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to establish a local user database for authentication.

 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.

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

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

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

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

```
Ruijie(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.

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

Related Commands	Command	Description
	login local	Enables local authentication

Platform Description N/A

2.46 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.

```
Ruijie# username import user.csv
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.47 username export

Use this command to export user information to the file.

username export filename

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

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 Examples	The following example exports user information to the file.	
Examples	<pre>Ruijie# username export user.csv</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.48 write

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

write [memory | terminal]

Parameter Description	Parameter	Description
	memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to copy running-config startup-config .
	terminal	Displays the system configuration, which is equivalent to show running-config .
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	<p>Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations.</p> <p>The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists;</p> <p>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, e.g., USB disk and SD</p>	

card, 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

```
Ruijie# write  
  
Building configuration...  
[OK]
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

3 Line Commands

3.1 absolute-timeout

Use this command to set the absolute timeout period. Use the **no** form of this command to restore the default setting.

absolute-timeout *minutes*
no absolute-timeout

Parameter Description	Parameter	Description
	<i>minutes</i>	Sets the absolute timeout period, in the range from 0 to 60.

Defaults No absolute timeout period is set by default.

Command Mode LINE configuration mode

Usage Guide If the absolute timeout period is configured, the line is disconnected once the timeout timer expires, Before the terminal logs out, a message is displayed to prompt the remaining time.

```
Terminal will be login out after 20 second
```

Configuration Examples The following example sets the timeout period for the line between two consoles to 2 minutes.

```
Ruijie(config)# line console 0
Ruijie(config-line)#absolute-timeout 2
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.2 accounting commands

Use this command to enable command accounting in the line. Use the **no** form of this command to restore the default setting.

accounting commands *level* { **default** | *list-name* }
no accounting commands *level*

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

<i>level</i>	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
default	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 command accounting first, and then apply it on the line.

Configuration Examples The following example enables command accounting in line VTY 1 and sets the command level to 15.

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
Ruijie(config)# line vty 1
Ruijie(config-line)# accounting commands 15 default
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.3 accounting exec

Use this command to enable user access accounting in the line. Use the **no** form of this command to restore the default setting.

accounting exec { default | list-name }

no accounting exec

Parameter Description	Parameter	Description
	default	
	<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 EXEC accounting first, and

then apply it on the line.

Configuration The following example enables user access accounting in line VTY 1.

Examples

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

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.4 activation-character

Use this command to set the ASCII value of the character for activating the terminal session. Use the **no** form of this command to restore the default setting.

activation-character *ascii-value*

no activation-character

**Parameter
Description**

Parameter	Description
<i>ascii-value</i>	Sets the ASCII value of the character for activating the terminal session, in the range from 0 to 127.

Defaults The default is CR (ASCII: 0x0D).

**Command
Mode** LINE configuration mode

Usage Guide If the current line is configured with the **autoselect** function, *ascii-value* must be set to 0x0D.

Configuration The following example configures Ctrl+Y (ASCII: 25) for activating the terminal session.

Examples

```
Ruijie(config)#line console 0
Ruijie(config-line)#activation-character 25
Ruijie(config-line)#end
Ruijie#exit

Press CTRL+y to get started

Ruijie>
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.5 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>	
default		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 The following example enables authorization on commands of level 15 in line VTY 1.

Examples

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.6 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
	default	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 EXEC authorization first, and then apply it on the line.

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

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.7 autocommand

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

autocommand *autocommand-string*

no autocommand

Parameter Description	Parameter	Description
	<i>autocommand-string</i>	Enables automatic command execution.

Defaults This function is disabled by default.

Command Mode LINE configuration mode

Usage Guide This command is used to enable the dumb terminal to log in to the specified host through Telnet or to obtain the specified app-based terminal service.

Configuration Examples The following example enables automatic command execution and connects to line vty 0.

```
Ruijie(config)# line vty 0
Ruijie(config-line)# autocommand telnet 192.168.21.100

//Initiates connection to line vty 0:
Trying 192.168.21.100, 23...

Ruijie#show users
Line          User          Host(s)          Idle          Location
-----
-----
0 con 0      ---          idle            00:01:31     ---
* 1 vty 0    ---          idle            00:00:00     192.168.21.200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.8 clear line

Use this command to clear connection status of the line.

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

Parameter Description	Parameter	Description
	console	Clears connection status of the console line.
	vty	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 Examples 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.

```
Ruijie# clear line vty 13
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.9 databits

Use this command to set the databit number for every character on the async line in flow communication mode. Use the **no** form of this command to restore the default setting.

databits *bit*

no databits

Parameter Description

Parameter	Description
<i>bit</i>	Sets the databit number of every character, in the range from 5 to 8.

Defaults The default is 8.

Command Mode LINE configuration mode

Usage Guide The async line device generates 7 databits with parity check in flow communication mode. If parity check is enabled, the databit number is 7. Otherwise, the databit number is 8. The databit number may set to 5 or 6 on the earlier device.

Configuration Examples The following example sets the databit number for every character on the async line in flow communication mode to 7.

```
Ruijie(config)# line console 0
Ruijie(config-line)# databits 7
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

3.10 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).

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# disconnect-character 5
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A

Description

3.11 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**).

```
Ruijie(config)# line vty 0
Ruijie(config-line)# escape-character 23
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.12 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

```
Ruijie(config)# line vty 1
Ruijie(config-line)# no exec
Ruijie# 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

3.13 exec-character-bits

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

exec-character-bits { 7 | 8 }

no exec-character-bits

**Parameter
Description**

Parameter	Description
7	Configures a 7-bit coded character set.
8	Configures an 8-bit coded character set.

Defaults The default is 8.

**Command
Mode** LINE configuration mode

Usage Guide If you want to enter Chinese characters in the command line or display Chinese characters, graphs or other international characters, configure the **exec-character-bits 8** command.

Configuration The following example configures a 7-bit coded character set for the async line.

Examples

```
Ruijie(config)# line console 0
Ruijie(config-line)#exec-character-bits 7
```

**Related
Commands**

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

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

Platform N/A
Description

3.14 flowcontrol

Use this command to configure the flow control mode for the async line. Use the **no** form of this command to restore the default setting.

flowcontrol { **hardware** | **none** | **software** }
no flowcontrol { **hardware** | **none** | **software** }

Parameter Description	Parameter	Description
	hardware	Configures hardware flow control.
none	Configures no flow control.	
software	Configures software flow control.	

Defaults No flow control is configured by default.

Command Mode LINE configuration mode

Usage Guide This command is used to control the data sending rate to make it consistent with the receiving rate at the receiving end. The terminal cannot receive data while sending data, so this function prevent s data drop. Flow control is also configured for the communication between high speed device and low speed device (for example, printer and network interface). RGOS provides two flow control modes, namely, software flow control and hardware flow control. The stop and start characters are Ctrl+S (XOFF, ASCII: 19) and Ctrl+Q (XON, ASCII: 17) respectively.

Configuration Examples The following example configures software flow control for the async line.

```
Ruijie(config)#line console 0
Ruijie(config-line)#flowcontrol software
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.15 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
	size <i>size</i>	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 Line configuration mode

Usage Guide N/A

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

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# history size 20
```

The following example disables the command history for line VTY 0 5.

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# no history
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.16 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. The value 0 means that there is no limit for screen length of the current line.
----------------------	-------------------------------------------------------------------------------------------------------------------------------------

Defaults The default is 24.

Command Mode Line configuration mode

Usage Guide N/A

Configuration The following example sets the screen length to 10.

Examples Ruijie(config-line)# length 10

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.17 line

Use this command to enter the specified LINE mode.

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

Parameter Description

Parameter	Description
console	Console port
vtty	Virtual terminal line, applicable for telnet/ssh connection.
<i>first-line</i>	Number of first-line to enter, in the range from 0 to 36.
<i>last-line</i>	Number of last-line to enter, int the range from first-line value+1 to 36.

Defaults N/A

Command Mode Global configuration mode

Usage Guide N/A

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

Examples Ruijie(config)# line vty 1 3

Related

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

Commands		
	N/A	N/A

Platform N/A

Description

3.18 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>	Number of VTY connections, in the range from 0 to 35.

Defaults N/A

Command Global configuration mode.

Mode

Usage Guide N/A

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

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

The following example decreases the number of available VTY connections to 10. The available VTY connections are numbered 0-9.

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

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.19 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>

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.

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

Related Commands	Command	Description
		N/A

Platform Description N/A

3.20 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

Defaults N/A

Command Mode Line configuration mode

Usage Guide N/A

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

```
Ruijie(config)# line vty 0 5
```

```
Ruijie(config-line)# monitor
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.21 parity

Use this command to configure the parity for the async line. Use the **no** form of this command to restore the default setting.

parity { even | none | odd }

no parity

Parameter Description	Parameter	Description
	even	Configures even parity.
	none	Configures no parity.
	odd	Configures odd parity.

Defaults No parity check is configured by default.

Command Mode LINE configuration mode

Usage Guide Parity is required in communication through some devices (such as async serial ports and console ports).

Configuration Examples The following example configures even parity for the async line.

```
Ruijie(config)#line console 0
Ruijie(config-line)#parity even
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.22 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 Examples The following example sets the privilege level for the line VTY 0 4 to 14.

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)privilege level 14
```

Related Commands	Command	Description
		N/A

Platform Description N/A

3.23 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>
	<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 ruijie device”.

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

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.24 show history

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

show history

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 command history of the line.

```
Ruijie# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.25 show line

Use this command to display line configuration.

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

Parameter Description	Parameter	Description
	console	
vty		Displays configuration for the virtual terminal line.
<i>line-num</i>		Displays the line.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

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

```
Ruijie# 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, AUX, TTY, 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 N/A
Description

3.26 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

```
Ruijie# show privilege
Current privilege level is 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.27 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 Examples The following example displays the information about users logging into the line,

```
Ruijie# 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,

```
Ruijie(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 --- 00:00:00 ---
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.28 start-character

Use this command to configure the start character for software flow control on the async line. Use the **no** form of this command to restore the default setting.

start-character *ascii-value*
no start-character

Parameter Description

Parameter	Description
<i>ascii-value</i>	Sets the ASCII value corresponding to the start character for software flow control on the async line, in the range from 0 to 255.

Defaults The default is Ctrl+Q (ASCII: 17).

Command Mode LINE configuration mode

Usage Guide The start character marks the start of the data transmission.

Configuration Examples The following example configures Ctrl+Y (ASCII: 25) for starting software flow control on the async line,

```
Ruijie(config)#line console 0
Ruijie(config-line)#start-character 25
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

3.29 stop-character

Use this command to configure the stop character for software flow control on the async line. Use the

no form of this command to restore the default setting.

stop-character *ascii-value*

no stop-character

Parameter Description	Parameter	Description
	<i>ascii-value</i>	Sets the ASCII value corresponding to the stop character for software flow control on the async line, in the range from 0 to 255.

Defaults The default is Ctrl+S (ASCII: 19).

Command LINE configuration mode

Mode

Usage Guide The stop character marks the end of the data transmission.

Configuration Examples The following example configures Ctrl+Z (ASCII: 26) for stopping software flow control on the async line,

```
Ruijie(config)#line console 0
Ruijie(config-line)#stop-character 26
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.30 stopbits

Use this command to configure the stopbit number for every character for the async line. Use the **no** form of this command to restore the default setting.

stopbits { 1 | 2 }

no stopbits

Parameter Description	Parameter	Description
	1	Configures 1 stopbit.
	2	Configures 2 stopbits.

Defaults The default is 2.

Command LINE configuration mode

Mode

Usage Guide The stopbit is required in communication between the async line and the async device (such as the conventional numb terminals and modems).

Configuration The following example sets the stopbit number of every character for the async line to 1.

```
Ruijie(config)#line console 0
Ruijie(config-line)#stopbits 1
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.31 terminal-type

Use this command to configure the simulated terminal type string of the async line.

terminal-type *terminal-type-string*

no terminal-type

Parameter Description	Parameter	Description
	<i>terminal-type-string</i>	Configures the terminal type string, such as vt100 and ansi.

Defaults The default is vt100.

Command Mode LINE configuration mode

Usage Guide You can use the **terminal-type vt100** command to restore the default terminal type. If you want to enable telnet connection, you should use the simulated terminal type to perform terminal type negotiation (Telnet: 0x18). See RFC 854 for details.

Configuration The following example sets the simulated terminal type of the async line to ansi.

```
Ruijie(config)#line console 0
Ruijie(config-line)#terminal-type ansi
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

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

```
Ruijie# terminal escape-character 23
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.33 terminal exec-character-bits

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

terminal exec-character-bits { **7** | **8** }

terminal no exec-character-bits

Parameter Description	Parameter	Description
	7	Configures a 7-bit coded character set.
	8	Configures an 8-bit coded character set.

Defaults The default is 8.

Command Mode Privileged EXEC mode

Usage Guide If you want to enter Chinese characters in the command line or display Chinese characters, graphs or other international characters, configure the **exec-character-bits 8** command.

Configuration The following example configures a 7-bit coded character set for the current terminal.

Examples

```
Ruijie#terminal exec-character-bits 7
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.34 terminal flowcontrol

Use this command to configure the flow control mode for the current terminal. Use the **no** form of this command to restore the default setting.

terminal flowcontrol { hardware | none | software }

terminal no flowcontrol { hardware | none | software }

Parameter Description	Parameter	Description
	hardware	
none		Configures no flow control.
software		Configures software flow control.

Defaults The default flow control mode is **none**.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example configures software flow control for the current terminal.

Examples

```
Ruijie#terminal flowcontrol software
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.35 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
	size <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.

```
Ruijie# terminal history size 20
```

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

```
Ruijie# terminal no history
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.36 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. The value 0 means that there is no limit for screen length of the current terminal.

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.

```
Ruijie# terminal length 10
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.37 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 "Swtich's Line Vty 0".

```
Ruijie# terminal location Swtich's Line Vty 0
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.38 terminal parity

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

terminal parity { even | none | odd }

terminal no parity

Parameter Description	Parameter	Description
	even	Configures even parity,
	none	Configures no parity.
	odd	Configures odd parity,

Defaults No parity check is configured by default.

Command Mode Privileged EXEC mode

Usage Guide Parity is required in communication through some devices (such as async serial ports and console ports).

Configuration Examples The following example configures even parity for the current terminal.

```
Ruijie#terminal parity even
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

3.39 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>

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,

```
Ruijie# terminal speed 115200
```

Related Commands	Command	Description
		N/A

Platform N/A

Description

3.40 terminal start-character

Use this command to configure the start character for software flow control on the current terminal.

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

terminal start-character *ascii-value*

terminal no start-character

Parameter Description	Parameter	Description
		<i>ascii-value</i>

Defaults The default is Ctrl+Q (ASCII: 17).

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures Ctrl+Y (ASCII: 25) for starting software flow control on the current device,

```
Ruijie#terminal start-character 25
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.41 terminal stop-character

Use this command to configure the stop character for software flow control on the current terminal.

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

terminal stop-character *ascii-value*

terminal no stop-character

**Parameter
Description**

Parameter	Description
<i>ascii-value</i>	Sets the ASCII value corresponding to the stop character for software flow control on the current terminal, in the range from 0 to 255.

Defaults The default is **Ctrl+S** (ASCII: 19).

**Command
Mode** Privileged EXEC mode

Usage Guide N/A

**Configuration
Examples** The following example configures **Ctrl+Z** (ASCII: 26) for stopping software flow control on the current device.

```
Ruijie#terminal stop-character 26
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

3.42 terminal stopbits

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

terminal stopbits { 1 | 2 }
terminal no stopbits

Parameter Description

Parameter	Description
1	Configures 1 stopbit,
2	Configures 2 stopbits.

Defaults The default is 2.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration Examples The following example configures 1 stopbit for the current terminal.

```
Ruijie#terminal stopbits 1
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

3.43 terminal terminal-type

Use this command to configure the simulated terminal type string for the current terminal. Use the **no** form of this command to restore the default setting.

terminal terminal-type *terminal-type-string*
terminal no terminal-type

Parameter Description

Parameter	Description
<i>terminal-type-string</i>	Sets the terminal type string.

Defaults The default is vt100.

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example sets the simulated terminal type string for the current terminal to ansi.

Examples `Ruijie#terminal terminal-type ansi`

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.44 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>

Defaults The default is 79.

Command Mode Privileged EXEC mode

Usage Guide N/A

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

`Ruijie# terminal width 10`

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.45 timeout login

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

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

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

3.46 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
	all	Allows all the protocols under Line to be used for communication
	ssh	Allows only the SSH protocol under Line to be used for communication
	telnet	Allows only the Telnet protocol under Line to be used for communication
	none	Allows none of protocols under Line to be used for communication

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

Command Line configuration mode

Mode

Usage Guide N/A

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

Examples

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

Related Commands

Command	Description
show running	Displays status information

Platform N/A

Description

3.47 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 Line configuration mode

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 ruijie device”.

Examples

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

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description**3.48 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
Examples**

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

```
Ruijie(config-line)# width 10
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

N/A

4 File System Commands

4.1 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 flash: , tmp: .
	<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 Mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples N/A

Related Commands	Command	Description
	pwd	Displays the present word directory.

Platform Description N/A

4.2 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 Privileged EXEC mode.

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
running-config	Running configuration file.
startup-config	startup configuration file.
flash:	local FLASH file system.
tftp:	The URL of TFTP network server, in the format as follows: tftp:[[/location]/directory]/filename
oob_tftp:	The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.

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.

```
Ruijie#copy tftp://192.168.64.2/netconfig flash:/netconfig

The file [flash:/netconfig] exists, override it? [Y/N]: y

Copying: !!!!!!!!

Accessing tftp://192.168.64.2/netconfig finished, 2399bytes prepared

Flushing data to flash:/netconfig...

Flush data done
```

Related Commands

Command	Description
delete	Deletes the file.
rename	Renames the file.
dir	Displays the file list of the specified directory.

Platform N/A

Description

4.3 delete

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

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

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

	includes flash: , usb: and tmp: .
<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 deletes the fstab file on the FLASH disk.

Examples

```
Ruijie#pwd
flash:/
Ruijie#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)
Ruijie#delete flash:/fstab
Ruijie#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)
```

Related Commands

Command	Description
copy	Copies the file.
dir	Displays the file list of the specified directory.

Platform N/A

Description

4.4 dir

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

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

Parameter	Parameter	Description
Description	<i>filesystem</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<i>file-url</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 N/A

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

Examples

```
Ruijie#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"> ● d: directory ● r: read ● w: write ● x: executable
10485760	File size
rpmdb	File name
files	File number
directories	Directory number
total	Total size
free	Available space

Related Commands	Command	Description
	pwd	Displays the present directory.

cd	Sets the present directory of the file system.
-----------	------------------------------------------------

Platform N/A
Description

4.5 mkdir

Use this command to create a directory.

mkdir [*filesystem:*] *directory*

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<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 Privileged EXEC mode.
Mode

Usage Guide N/A

Configuration The following example creates a directory named newdir:

```

Examples
Ruijie#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)
Ruijie#mkdir newdir
Created dir flash:/newdir
Ruijie#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	Command	Description
---------	---------	-------------

Commands	rmdir	Deletes the directory.
	pwd	Displays the present directory.

Platform N/A

Description

4.6 more

Use this command to display the content of a file.

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

	Parameter	Description
Parameter Description	/ascii	Displays the file content in the ASCII format.
	/binary	Displays the file content in the
	filesystem:	The URL of file system, followed by a colon (:). The file system includes flash: , sd: and tmp: .
	file-url	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 Privileged EXEC mode

Mode

Usage Guide N/A

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

```

Examples
Ruijie#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

4.7 pwd

Use this command to display the working path.

pwd

Parameter	Parameter	Description
Description	N/A	N/A

Defaults N/A

Usage Guide N/A

Configuration N/A

Examples

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

Platform N/A

Description

4.8 rename

Use this command to move or rename the specified file.

rename *src-url dst-url*

Parameter	Parameter	Description
Description	<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 Privileged EXEC mode.
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

```
Ruijie#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)
Ruijie#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
Ruijie#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
	delete	Deletes the file.
	copy	Copies the file.

Platform N/A

Description

4.9 rmdir

Use this command to delete an empty directory.

rmdir [*filesystem:*] *directory*

Parameter Description	Parameter	Description
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<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 Privileged EXEC mode.

Usage Guide N/A

Configuration The following example deletes the null test directories.

Examples

```
Ruijie#mkdir newdir
Ruijie#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)
Ruijie#rmdir newdir
removed dir flash:/newdir
Ruijie#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

4.10 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/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the file system information:

Examples

```
Ruijie#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:
```

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"> ● ro: read-only ● wo: write-only ● rw: read and write
Prefixes	File system prefix

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.11 show mount

Use this command to display the mounted information.

show mount

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration Examples The following example displays the mounted information.

```
Ruijie#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

4.12 tree

Use this command to display the file tree of the current directory.

tree [*filesystem:*] [*directory*]

Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , tmp: .
	<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 User EXEC mode/Privileged EXEC mode

Mode**Usage Guide** N/A**Configuration** The following example displays the file tree of flash:/echo**Examples**

```
Ruijie#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 Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.13 verify

Use this command to compute, display and verify Message Digest 5 (MD5).

verify [/md5 md5-value] filesystem: [file-url]

Parameter	Parameter	Description
Description	/md5	Computes and displays MD5.
	md5-value	The file MD5, which is compared with the computed MD5.
	filesystem:	The URL of file system, followed by a colon (:). The file system includes flash: , tmp: .
	file-url	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 Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example computes MD5 of flash:/gcc.

```
Ruijie#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

The following example computes MD5 and makes a comparison.

```
Ruijie#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying /mnt/flash/gcc = 8b072de7db7affd8b2ef824e7e4d716c
Ruijie#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

5 SYS Commands

5.1 calendar set

Use this command to set the hardware calendar.

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 2037.


Defaults N/A

Command Mode Privileged EXEC mode

Default Level 1

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".
- If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward. For example, February 2012 has 29 days. If you use the **calendar set 11:30 2 31 2012** command to set the date to February 31, by default, the system adds two days backwards. Therefore, the current hardware time is "2012-03-02 11:30:23".

 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.

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.


```
Ruijie# 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.

```
Ruijie# 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.

```
Ruijie# 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).

Check Method N/A

Platform Description N/A

5.2 clock read-calendar

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

clock read-calendar

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 1

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

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

Check Method N/A

Platform N/A

Description

5.3 clock set

Use this command to set the system software 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 2037.

Defaults N/A


Command Mode Privileged EXEC mode

Default Level 1

Usage Guide 1. 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".

2. If the value of parameter *day* is between 1 and 31, but the current month does not contain that day, the value will be calculated backward.

 For example, February 2012 has 29 days. If you use the **clock set 11:30 2 31 2012** command to set the date to February 31, by default, the system adds two days backward. Therefore, the current hardware time is "2012-03-02 11:30:23".

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.

```
Ruijie# 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.

```
Ruijie# 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.

```
Ruijie# 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).

Check Method N/A

Platform Description N/A

5.4 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
	N/A	N/A

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 1

Usage Guide This command is supported only in vsd0. 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.

```
Ruijie# 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.

```
Ruijie# show clock
```

```
09:30:21 TSZ Wed, Feb 29, 2012

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

Ruijie#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.

```
Ruijie# show clock
09:30:02 TSZ Wed, Feb 29, 2012

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

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

Check Method N/A

Platform N/A
Description

5.5 cpu high-watermark set

Use this command to set the threshold of CPU usage and enable CPU usage monitoring.

cpu high-watermark set [[**up** *up-value*] [**down** *down-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
	up <i>up-value</i>	Sets the high threshold of the CPU usage. The range is from 1% to 99%.
	down <i>down-value</i>	Sets the low threshold of the CPU usage. The range is from 1% to 99%.

Defaults By default, the high threshold and low threshold are 85% and 75% respectively.

Command Mode Global configuration mode

Default Level 15

Usage Guide This command is supported only in vsd0.
 You can use this command to set the threshold of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the threshold, the system prints prompts.

Configuration Examples The following example sets the CPU usage threshold to the default value and enables CPU usage monitoring (if it is disabled).

```
Ruijie(config)# default cpu high-watermark set
Reset default cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

The following example disables CPU usage monitoring.

```
Ruijie(config)# no cpu high-watermark set
Close cpu watermark monitor
```

The following example enables CPU usage monitoring. Keep the defined threshold value.

```
Ruijie(config)# cpu high-watermark set
Open cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

The following example sets the high threshold and low threshold of CPU usage to 90% and 70% respectively.

```
Ruijie(config)# cpu high-watermark set up 90 down 70
Open cpu watermark monitor
Set system cpu high-watermark up 90%, down 70%
```

Check Method N/A

Prompt Message If the high threshold 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 high threshold.

```
*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 lower than the high threshold, 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 N/A
Description

5.6 memory low-watermark set

Use this command to set the threshold of memory usage and enable memory usage monitoring.

memory low-watermark set *mem-value*

Use the **no** form of this command to disable memory usage monitoring.

no memory low-watermark

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

Defaults By default, the memory usage threshold is 90%.

Command Mode Global configuration mode

Default Level 15

Usage Guide You can use this command to set the memory usage threshold and enable monitoring.

Configuration Examples The following example sets the memory usage threshold to 80% and enables monitoring.

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

Check Method N/A

Prompt Message N/A

Platform Description N/A

5.7 memory history clear

Use this command to clear the history of the memory usage.

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

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

Description	
one-forth	Clears one fourth entries.
half	Clears a half of entries.
all	Clears all the entries.

Defaults N/A

Command Mode Global configuration mode

Default Level 15

Usage Guide N/A

Configuration The following example clears a half of the history of the memory usage.

Examples

```
Ruijie# show memory history

Time Thu Jan 1 00:24:45 1970
Used(k) 148516
Maxinum 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
Maxinum 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
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      44088
rg_syslogd      36640

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

Check Method N/A

Prompt Message N/A

Platform Description N/A

5.8 reload

Use this command to reload the device.

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

Parameter Description

Parameter	Description
<i>hour</i> [: <i>minute</i> [: <i>second</i>]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
<i>month</i>	Sets the month, in the range from 1 to 12.
<i>day</i>	Sets the day, in the range from 1 to 31.
<i>year</i>	Sets the year, in the range from 1970 to 2099.

Defaults N/A

Command Mode Privileged EXEC mode

Default Level 15

Usage Guide N/A

Configuration Examples The following example reloads the device.

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

Check Method N/A

Prompt Message N/A

Platform N/A

Description

5.9 show calendar

Use this command to display the hardware calendar.

show calendar

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 1

Usage Guide N/A

Configuration Examples The following example displays the hardware calendar.

```
Ruijie# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

Prompt Message N/A

Platform Description N/A

5.10 show clock

Use this command to display the system software clock.

show clock

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode / global configuration mode

Default Level 1

Usage Guide N/A

Configuration The following example displays the software clock when the time zone is disabled.

Examples

```
Ruijie# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

The following example displays the software clock when the time zone is enabled.

```
Ruijie# show clock
03:07:49 TSZ Wed, Feb 29, 2012
```

Prompt Message N/A

Platform Description N/A

5.11 show memory

Use this command to display the system memory.

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

Parameter Description	Parameter	Description
	sorted total	Ranked according to the memory usage.
	history	Displays the history of memory usage.
	low-watermark	Displays the memory low watermark threshold of the system.
	<i>process-id</i>	Displays the memory usage of the task specified by <i>process-id</i> , in the range from 0 to 32768.
	<i>process-name</i>	Displays the memory usage of the task specified by <i>process-name</i> .

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 15

Usage Guide Every time when the **show memory history** command is used, the number of displayed entries increases by one. Up to 10 entries can be displayed. You can use the **memory history clear** command to clear history entries.

Configuration Examples The following example displays the memory usage of each task and the ranking (based on the total memory usage).

```
Ruijie# show memory sorted total
System Memory: 508324K total, 481560K used, 26764K free, 31.5% used rate
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--

Keyword	Description
total	Total system memory
used	Used memory
free	Remaining memory
used rate	Memory usage (percentage)
Active	Active page
inactive	Inactive page
mapped	Mapped memory
slab	Memory consumed by Slab
others	Memory capacity of the used memory except the memory used 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

Prompt Message N/A

Platform Description N/A

5.12 show memory vsd

Use this command to display memory information.

show memory vsd vsd_id

Parameter Description	Parameter	Description
	<i>vsd_id</i>	VSD ID is a digit. You can use the show vsd command to display the ID of each VSD. The ID range is from 0 to 16.
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	15	

Usage Guide  This command is supported only in VSD0 mode.

Configuration Examples The following example displays the memory usage of each task in VSD 1 mode.

```
Ruijie#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
1348     1316    4656    1004    84      10764   isis.elf
1347     212     4220    872     84      9368    ripng.elf
1345     460     4284    876     84      9656    rip.elf
1344     1800    5568    1572    84      12156   bgp.elf
1340     1084    4700    1024    84      10928   ldp.elf
1339     288     17684   556     84      21472   msf.elf
```

```
1338    208    3604    42712   84    47708   rg-syslogd
--More--
```

Prompt
Message N/A

Platform
Description N/A

5.13 show pci-bus

Use this command to display the information on the device mounted to the PCI bus.

show pci-bus

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode/global configuration mode

Default Level 1

Usage Guide N/A

Configuration Examples The following example displays the information on the device mounted to the PCI bus.

```
Ruijie# 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
    
```

Prompt Message N/A

Platform Description N/A

5.14 show processes cpu

Use this command to display system task information.

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

Parameter Description	Parameter	Description
	5sec 1min 5min 15min	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
	nonzero	Does not display the task with 0 CPU usage.
	history	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
	table	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 15

Usage Guide This command is supported only in vsd0.

Configuration Examples The following example displays the tasks listed in ascending order of task IDs.

```

Ruijie# 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 the tasks listed in ascending order of task IDs without displaying the tasks with 0 CPU usage within 15 minutes.

```
Ruijie# show processes cpu nonzero
```

Field	Description
System Uptime	Total running time of the device, precious to seconds.
CPU Utilization	Total CPU usage of the control core within the last five seconds, one minute, and five minutes.
Virtual CPU usage	Total CPU usage of the virtual control core within the last five seconds, one minute, and five minutes.
Tasks Statistics	Task statistics information, including the total number of statistics tasks and the task status.
set system cpu watermark	CPU watermark value and status of the control core.

The task running statuses are listed below:

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

Description of each task:

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

The following example displays the CPU usage in ascending order of task IDs and only the processes with non-zero CPU usage within 15 minutes are displayed.

```
Ruijie #show processes cpu nonzero
```

The following example displays the CPU usage in descending order within five seconds and the tasks with zero CPU usage within one second are not displayed.

```
Ruijie #show processes cpu 5sec nonzero
```

The following example displays the CPU usage of the control core in histograms within the last 60 seconds, 60 minutes, and 72 hours.

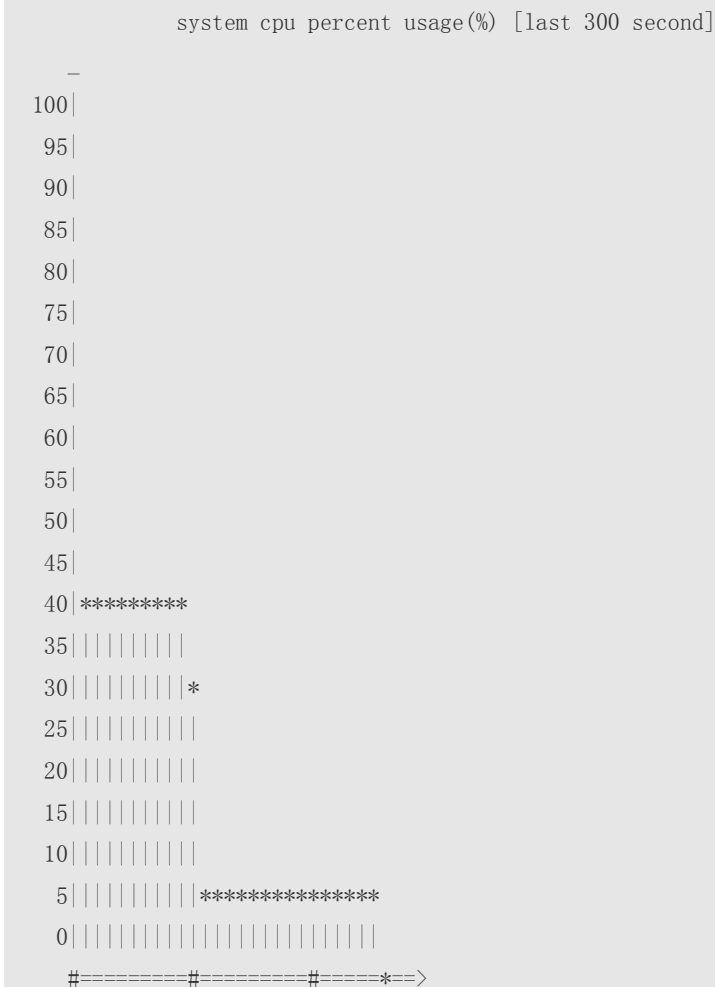
The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate nearest to 0 is the CPU usage in the last five seconds, measured in %.

The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

The third histogram displays the CPU usage of the control core within the last 72 hours, measured in %. Every segment on the x-coordinate is 1 hour.

Example:

```
Ruijie#show processes cpu history
```



```

0      50      100      second
system cpu percent usage(%) per 5second (last 125 second)
-----

system cpu percent usage(%) [last 60 minute]

-
100|
95 |
90 |
85 |
80 |
75 |
70 |
65 |
60 |
55 |
50 |
45 |
40 |
35 |
30 |*
25 | |
20 | |
15 | |
10 | |
5  | |*
0  | | |
#==*==>
0      minute
system cpu percent usage(%) per 1minute (last 2 minute)
-----

```

The following example displays the CPU usage of the core 0 in tables within the last 60 seconds, 60 minutes, and 72 hours.

The first table lists the CPU usage within the last 300 seconds. The first cell indicates the CPU usage within the last five seconds.

The second table lists the CPU usage within the last 60 minutes, measured in %. The two adjacent cells show the CPU usage measured at an interval of one minute.

The third table lists the CPU usage within the last 72 hours, measured in %. The two adjacent cells show the CPU usage measured at an interval of one hour.

Example:

```

Ruijie #show processes cpu history table
system cpu percent usage(%) [last 300 second]
#-----#

```

```

|      | 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 |
#-----#

```

Prompt Message N/A

Platform Description N/A

5.15 show processes cpu detailed

Use this command to display the details of the specified task.

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

Parameter Description	Parameter	Description
	<i>process-id</i>	Displays the information on the task of the specified task ID.
	<i>process-name</i>	Displays the information on the task of the specified task name.

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 15

Usage Guide This command is supported only in vsd0.

Configuration The following example displays the information on the task of the specified task name.

Examples

```
Ruijie# 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      :
  Lass 5 sec   0.3% (0.6%)
  Lass 1 min   0.3% (0.6%)
  Lass 5 min   0.3% (0.6%)
  Lass 15 min  0.3% (0.6%)
Tty            : ?
```

i Code Usage: 209.6 KB. If the specified task name is not unique, the system displays the following message:

```
Ruijie# 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	VSD ID of the task
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 for the task from self-startup to now
Run Time	Duration for the task from self-startup to being executed

Cpu Usage	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%).
Tty	Tty ID, in the format of "Primary device ID, secondary device ID". If it is 0, the value is ?.
Code Usage	Size occupied by the task code segment

The following example displays the information on the task of the specified task ID.

```
Ruijie# show process cpu detailed 1715
```

Prompt Message N/A

Platform Description N/A

5.16 show version

Use this command to display the system version information.

show version

Parameter Description	Parameter	Description
	-	-

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 1

Usage Guide N/A

Usage Guide The following example displays the system version information.

```
Ruijie# show version
System description      : Ruijie Gibabit Ethernet Switch(XS-S1930J-48GT4SFP) By Ruijie Networks
System start time      : 2020-11-30 17:59:16
System uptime          : 7:20:57:39
System hardware version : 1.00
System software version : S1930J_RGOS 11.4(1)B70P10, Release(07233016)
System patch number    : NA
System serial number    : 1234942570074
System boot version     : 2011.12. (3.6.2)
```

```
Module information:
Slot 0 : XS-S1930J-48GT4SFP
  Hardware version   : 1.00
  Boot version      : 2011.12. (3.6)
  Software version   : S1930J_RGOS 11.4(1)B70P10, Release(07233016)
  Serial number     : 1234942570074
```

Prompt Message N/A

Platform Description N/A

5.17 show cpu

Use this command to display the information on the system task running on the control core instead of the non-virtual core.

show cpu

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode/ global configuration mode

Default Level 15

Usage Guide This command is supported only in vsd0.
If the system is equipped with a virtual core, you can use the **show processes cpu** command to check the CPU usage of the virtual core.

Configuration Examples The following example displays the information on the system task running on the control core instead of the non-virtual core.

```
Ruijie#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--
    
```

Prompt Message N/A

Platform Description N/A

5.18 show reboot-reason

Use this command to display the reboot reason.

show reboot-reason

Parameter Description	Parameter	Description
	N/A	N/A

Command Mode Privileged EXEC mode/ global configuration mode/ User EXEC mode

Default Level N/A

Usage Guide N/A

Configuration Examples The following example displays the reboot reason of the device.

```

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

Ruijie#
    
```

Prompt Message N/A

Platform Description N/A

6 Time Range Commands

6.1 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
	start <i>time date</i>	Indicates the start time of the range.
	end <i>time date</i>	Indicates the end time of the range.

Defaults No absolute time range is configured by default.

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.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures an absolute time range.

```
Ruijie(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 N/A

Platform Description N/A

6.2 periodic

Use this command to configure 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. It is recommended to disassociate time range before you change the periodic time and associate it again after you change the periodic time.

Configuration Examples The following example creates a time range and enters time range configuration mode.

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

The following example configures a periodic time interval.

```
Ruijie(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 N/A

Platform Description N/A

6.3 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>

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

```
Ruijie# show time-range
time-range entry: test (inactive)
  absolute end 01:02 02 February 2012
```

Prompt Message N/A

Platform Description N/A

6.4 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>

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

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

Check Method Use the **show time-range** [*time-range-name*] command to display the time range configuration.

Prompt Message N/A

Platform Description N/A

7 HTTP Service Commands

7.1 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 | default } enable service web-server [http | https | all]

Parameter Description

Parameter	Description
http	Enables the HTTP service.
https	Enables the HTTPS service.
all	Enables both the HTTP service and the HTTPS service.

Defaults

By default, HTTP and HTTPS are 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 and HTTPS service.

Use the command **no enable service web-server** or **default enable service web-server** to disable the corresponding HTTP service.

Configuration

The following example enables both the HTTP and HTTPS service:

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#enable service web-server
```

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

7.2 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 Examples The following example configures the HTTP port number as 8080:

```
Ruijie(config)#http port 8080
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

7.3 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 HTTP port number. The value includes 443 and the range from 1025 to 65,535.

Defaults The default HTTPS 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

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#http secure-port 4443
```

Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.
	show web-server status	Displays the configuration and status of the Web service.

Platform N/A

Description

7.4 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 The following example displays the configuration and status of the Web service:

Examples

```
Ruijie#show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
```

Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.
	http server port	Configures the HTTP port number.
	https server port	Configures the HTTPS port number.

Platform N/A
Description

7.5 upgrade web

Use this command to upgrade the Web package in local file system.

upgrade web *uri*

Parameter Description	Parameter	Description
	<i>uri</i>	The storage path of the Web package.

Defaults N/A

Command mode Privileged EXEC mode

Usage Guide Please use the **copy** command to copy the Web package into the file system before you use this command to upgrade the Web package.

Configuration Examples The following example copies a Web package into the file system and upgrades the package.

```
Ruijie#copy tftp://192.168.23.24/web.upd flash:/web.upd
Ruijie#upgrade web flash:/web.upd
```

Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.

Platform N/A
Description

7.6 upgrade web download

Use this command to download the Web package from the TFTP server and upgrade the package automatically.

upgrade web download tftp: *path*

Parameter Description	Parameter	Description
	tftp: <i>path</i>	<i>path</i> indicates the storage path of the Web package on the TFTP server. tftp indicates the system downloads the Web package from the TFTP

	server through the physical port and upgrades the Web package automatically.
--	------------------------------------------------------------------------------

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration Examples The following example downloads a Web package from the TFTP server and upgrades the package automatically.

```
Ruijie#upgrade web download tftp://192.168.23.24/web.upd
```

Related Commands	Command	Description
		enable service web-server

Platform Description N/A

7.7 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>
	<i>name</i>	Username.
	<i>password</i>	Password.
	0 7	Password type; 0 indicates plaintext, 7 indicates ciphertext.
	<i>encrypted-password</i>	Password text.

Defaults By default, two users are configured.


1. User1 is configured with privilege level 1, username of admin and plaintext password of admin.
2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.

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.

Configuration The following example configures the username and password for Web login authentication,

Examples

```
Ruijie(config)#webmaster level 0 username ruijie password admin
```

Related Commands

Command	Description
enable service web-server	Enables the HTTP service.

Platform N/A

Description

8 Syslog Commands

8.1 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 Examples The following example clears the log packets from the memory buffer.

```
Ruijie# clear logging
```

Related Commands	Command	Function
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	logging buffered	Records the logs in the memory buffer.

Platform Description N/A

8.2 logging

Use this command to send the log message to the specified syslog server.

logging { ip-address } [udp-prot port]

Use this command to delete the specified syslog server.

no logging { ip-address } }

Use this command to restore the default port 514.

no logging { ip-address } udp-prot

Parameter	Parameter	Description
Description		

<i>ip-address</i>	Sets the IP address of the host receiving log messages.
udp-port <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 The following example configures a syslog server with IP address 202.101.11.1.

Examples

```
Ruijie(config)# logging 202.101.11.1
```

The following example configures a syslog server with IP address 10.1.1.100 and port number 8099.

```
Ruijie(config)# logging 202.101.11.1 udp-port 8099
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.3 logging buffered

Use this command to set the memory buffer parameters (log severity, 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>	Size of the buffer is related to the specific device type: For the access switches, 4 K to 1 M Bytes.
<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 related to the specific device type.
access switches: 128 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

```
Ruijie(config)# logging buffered 10000 6
```

Related

Commands

Command	Description
logging on	Turns on the log switch.
show logging	Displays the logs in the buffer.
clear logging	Clears the logs in the log buffer.

Platform
Description N/A

8.4 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
Description	<i>level</i>	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used.

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.

Keyword	Severity Level	Description
Emergencies	0	System is unusable
Alerts	1	Immediate action needed
Critical	2	Critical conditions
Errors	3	Error conditions
Warnings	4	Warning conditions
Notifications	5	Normal but significant conditions
Informational	6	Informational messages
Debugging	7	Debugging messages

Configuration Examples The following example sets the severity of log that is allowed to be displayed on the console as 6:

```
Ruijie(config)# logging console informational
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs and related log configuration parameters in the buffer.

Platform N/A

Description

8.5 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 Examples The following example enables the log statistics function:

```
Ruijie(config)# logging count
```

Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.6 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

Parameter	Parameter	Description
Description	<i>facility-type</i>	Syslog device value. For specific settings, refer to the usage

	guide.
--	--------

Defaults The default is 16 if the RFC5424 format is enabled (Local0, local use).
 The default is 23 if the RFC5424 format is disabled (Local7, local use).

Command Mode Global configuration mode

Usage Guide The following table 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 Examples The following example sets the device value of **Syslog** as **kernel**:

```
Ruijie(config)# logging facility kern
```


Related Commands	Command	Description
	logging console	Sets the severity of logs that are allowed to be displayed on the console.

Platform Description N/A

8.7 logging file

Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH or USB. Use the **no** form of this command to restore the default setting,

logging file flash:filename [max-file-size] [level]


no logging file

Parameter Description	Parameter	Description
	flash	Saves the log file in expanded FLASH.
	<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.

 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.

```
Ruijie(config)# logging file flash:syslog
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.8 logging file numbers

Use this command to set the number of log files written into FLASH. Use the **no** form of this command to restore the default setting.

- logging file numbers** *numbers*
- no logging file numbers**

Parameter Description

Parameter	Description
<i>numbers</i>	Sets the number of log files written into FLASH, in the range from 2 to 32.

Defaults The default is 16.

Command Mode Global configuration mode

Usage Guide The system does not delete previously generated log files even if you change this configuration, Therefore, you need to delete the log files manually to save FLASH size (you can send log files to the server through TFTP before that). For example, 16 log files are generated by default before you want to change the number to 2. New logs are overwritten constantly in log files indexed 0 to 1. However, log files indexed from 2 to 16 remain. You can delete these log files manually as needed.

Configuration Examples The following example sets the number of log files written into FLASH to 8.

```
Ruijie(config)# logging file numbers 8
```

Related Commands	Command	Description
	N/A	N/A

Platform
Description

N/A

8.9 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
Mode

Global configuration 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 Ruijie(config)# logging flash flush

Related Commands	Command	Description
	N/A	N/A

Platform
Description

N/A

8.10 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

Parameter Description	Parameter	Description
	interval <i>seconds</i>	The interval to write log messages into the flash file, in the range from 1 to 51840 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 Examples The following example sets the interval to write log messages into the flash file to 300 seconds.

```
Ruijie(config)# logging flash interval 300
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.11 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
	all	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
	buffer	Log messages destined to the log buffer are filtered, including log messages displayed by running the show logging command.
	file	Log messages destined to the log file are filtered.
	server	Log messages destined to the log server are filtered.

terminal	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 Global configuration mode

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).

```
Ruijie(config)# logging filter direction terminal
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.12 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
contains-only	The log message containing the key word of the filter rule is printed.
filter-only	The log message containing the key word of the filter rule is filtered.

Defaults The default filter type is filter-only.



Command Global configuration mode

Mode

Usage Guide

1. 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,
2. 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 The following example sets the filter type to contains-only.

Examples Ruijie(config)# logging filter type contains-only

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

8.13 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
exact-match	Exact-match filter rule. Fill in all the following three parameters.
single-match	Single-match filter rule. Fill in one of the following three parameters.
module <i>module-name</i>	Module name.
mnemonic <i>mnemonic-name</i>	Mnemonic name.
level <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.

```
Ruijie(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.

```
Ruijie(config)# logging filter rule single-match module SYS
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

8.14 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 in the range from 0 to 7.
<i>days</i>	Sets the preservation duration of logs in the range from 7 to 365.

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 The following example sets the preservation duration of logs whose level is 6 to 10 days.

Examples Ruijie(config)# logging life-time level 6 10

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

8.15 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	Parameter	Description
Description	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used.

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.

Keyword	Severity Level	Description
Emergencies	0	System is unusable
Alerts	1	Immediate action needed
Critical	2	Critical conditions
Errors	3	Error conditions
Warnings	4	Warning conditions
Notifications	5	Normal but significant conditions
Informational	6	Informational messages
Debugging	7	Debugging messages

Configuration The following example sets the severity of log that is allowed to be printed on the VTY window as 6:

Examples `Ruijie(config)# logging monitor informational`

Related Commands	Command	Description
		<code>logging on</code>
	<code>show logging</code>	Displays the log messages and related log configuration parameters in the buffer.

Platform N/A

Description

8.16 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

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 equipments 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 greater than 1.

Configuration The following example disables the log switch on the device.

Examples `Ruijie(config)# no logging on`

Related Commands	Command	Description
	<code>logging buffered</code>	Records the logs to a memory buffer.
	<code>logging server</code>	Sends logs to the Syslog server.
	<code>logging file flash:</code>	Records logs on the expanded FLASH.
	<code>logging console</code>	Allows the log level to be displayed on the console.
	<code>logging monitor</code>	Allows the log level to be displayed on the VTY window (such as telnet window) .

logging trap	Sets the log level to be sent to the Syslog server.
---------------------	-----------------------------------------------------

Platform
Description N/A

8.17 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	Parameter	Description
Description	<i>number</i>	The number of logs that can be processed in a second in the range from 1 to 10000.
	all	Sets rate limit to all the logs with severity level 0 to 7.
	console	Sets the amount of logs that can be shown in the console in a second.
	except	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 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:

```
Ruijie(config)#logging rate-limit all 10 except warnings
```

Related	Command	Description
Commands	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform
Description N/A

8.18 logging server

Use this command to send the logs to the specified Syslog Server 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* } [**udp-prot** *port*]

no logging server { *ip-address* }

no logging server { *ip-address* } **udp-prot**

Parameter	Parameter	Description
Description	<i>ip-address</i>	IP address of the host that receives log information.
	udp-prot <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 Ruijie(config)# **logging server** 202.101.11.1

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays log messages and related log configuration parameters in the buffer.
	logging trap	Sets the level of logs allowed to be sent to Syslog server.

Platform Description N/A

8.19 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 Examples The following example specifies loopback 0 as the source address of the syslog messages:

```
Ruijie(config)# logging source interface loopback 0
```

	Command	Description
Related Commands	logging server	Sends logs to the Syslog server.

Platform Description N/A

8.20 logging source ip

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 }

no logging source { ip }

	Parameter	Description
Parameter Description	<i>ip-address</i>	Specifies the source IPv4 address sending the logs to IPv4 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

```
Ruijie(config)# logging source ip 192.168.1.1
```

Related Commands	Command	Description
	logging server	Sends the logs to the Syslog server.

Platform Description N/A

8.21 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 Description	Parameter	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 The following example enables synchronization function.

Examples

```
Ruijie(config)#line console 0
Ruijie(config-line)#logging synchronous
```

Print UP-DOWN logs on the port when keying in the command, the input command will be output again:

```
Ruijie# 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
Ruijie# configure terminal//----the input command by the user is output
again rather than being intererupted.
```

Related Commands	Command	Description
	show running-config	Displays the configuration.

Platform Description N/A

8.22 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 Description	Parameter	Description
	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used.

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.

Keyword	Severity Level	Description
Emergencies	0	System is unusable
Alerts	1	Immediate action needed
Critical	2	Critical conditions
Errors	3	Error conditions
Warnings	4	Warning conditions
Notifications	5	Normal but significant conditions
Informational	6	Informational messages
Debugging	7	Debugging messages

Configuration The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22:

Examples

```
Ruijie(config)# logging 202.101.11.22
Ruijie(config)# logging trap informational
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	logging	Sends logs to the Syslog server.
	show logging	Displays the log messages and related log configuration parameters in the buffer.

Platform N/A
Description

8.23 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 Description	Parameter	Description
	N/A	N/A

Defaults No log message is printed recording user log/exit by default.

Command Global configuration mode
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 The following example enables the logging function to record user log/exit.

Examples Ruijie(config)# logging userinfo

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

8.24 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 No 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.

```
Ruijie(config)# logging userinfo command-log
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.25 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	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

```
Ruijie(config)# service log-format rfc5424
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

8.26 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 Ruijie(config)# service private-syslog

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

8.27 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 The following example adds serial numbers to the logs.

Examples Ruijie(config)# **service sequence-numbers**

Related Commands	Command	Description
	logging on	Turns on the log switch.

service timestamps	Attaches timestamps to the logs.
---------------------------	----------------------------------

Platform N/A
Description

8.28 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 Examples The following example sets the standard syslog format.

```
Ruijie(config)# service standard-syslog
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

8.29 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	Parameter	Description
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
Ruijie #config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie (config)#service sysname
Ruijie (config)#end
Ruijie #
Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console
    
```

Related	Command	Function
Commands	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description N/A

8.30 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	Parameter	Description
Description	<i>message-type</i>	The log type, including Log and Debug . The log type indicates the log information with severity levels of 0 to 6. The debug type indicates that with severity level 7.
	uptime	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41.
	datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
	msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299.
	year	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.

```
Ruijie(config)# service timestamps debug datetime msec
Ruijie(config)# service timestamps log datetime msec
Ruijie(config)# end
Ruijie(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console
by console
```

Related Commands	Command	Description
	logging on	Turns on the log switch.
	service sequence-numbers	Enables serial numbers of logs.

Platform Description N/A

8. 31 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	Parameter	Description
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.

```
Ruijie# 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: Ruijie %LINK-3-UPDOWN: Interface GigabitEthernet
0/1, changed state to up.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet 0/1, changed state to up.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface GigabitEthernet
0/24, changed state to down.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTON/A5N/AUPDOWN: Line protocol on
Interface GigabitEthernet 0/1, changed state to down.
```

```
015491: *Sep 19 02:46:28: Ruijie %LINKN/A3N/AUPDOWN: Interface
GigabitEthernet 0/1, changed state to up.
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet 0/1, 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** command with RFC5424 format enabled.

```
Ruijie# 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 ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881
name="" type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z ruijie 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
logging on	Turns on the log switch.
clear logging	Clears the log messages in the buffer.

Platform Description

N/A

8.32 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.

```
Ruijie# 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.

```
Ruijie# 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

8.33 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	Parameter	Description
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 The following example displays the result of the **show logging count** command:

```

Examples
Ruijie# 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
	logging count	Enables the log statistics function.
	show logging	Displays basic configuration of log modules and log information in the buffer.
	clear logging	Clears the logs in the buffer.

Platform Description N/A

8.34 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 N/A

Configuration Examples The following command displays the result of the **show logging reverse** command with RFC5424 format disabled.

```
Ruijie# 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: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet 0/1, changed state to up.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface GigabitEthernet
0/1, changed state to up.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet 0/1, changed state to down.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface GigabitEthernet
0/24, changed state to down.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet 0/1, changed state to up.
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface GigabitEthernet
0/1, 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.

```
Ruijie# 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 ruijie SYS 6 SHELL_CMD [USER@4881
name=""][CMD@4881 task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881 name=""
type="" from="console"] user login success.
```

```
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address
for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address
for capwap.
<135>1 2013-07-24T12:19:33.130290Z ruijie - 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

8.35 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 The following example allows log information to be printed on the current VTY window:

Examples Ruijie# terminal monitor

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

Command History	Version	Description
	N/A	N/A

9 CWMP Commands

9.1 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-type 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-type</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-type: 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.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs password 123
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
------------------	---------	-------------

show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Platform N/A

Description

9.2 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 CWMP configuration mode

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 256 characters.

Configuration The following example specifies the URL of the ACS to <http://10.10.10.1:7547/acs>.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://10.10.10.1:7547/acs
Ruijie(config-cwmp)#
```

The following example specifies the URL of the ACS to `http://www.test.com/service/tr069servlet`.

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://www.test.com/service/tr069servlet
```

```
Ruijie(config-cwmp) #
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.3 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
no acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.

Defaults N/A

Command Mode CWMP configuration 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.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs username admin
Ruijie(config-cwmp) #
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
acs password	Configures the ACS password to be authenticated for the CPE to connect to the

	ACS.
--	------

Platform N/A
Description

9.4 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 10,000 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.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.5 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 Mode CWMP configuration 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 Examples The following example specifies the periodical notification interval of the CPE to 60 seconds.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe inform interval 60
```

```
Ruijie(config-cwmp) #
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.6 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-type 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-type</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-type: 0
 encrypted-password: N/A

Command Mode CWMP configuration 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:

-  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 CPE password to be authenticated for the ACS to connect to the CPE to 123.

```
Ruijie#config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe password 123
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
	acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.

Platform N/A

Description

9.7 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.

Defaults N/A

Command CWMP configuration mode

Mode

Usage Guide Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements:

- The URL of the CPE is formatted as `http://ip [: port]/ path`.
- The URL of the CPE consists of at most 256 characters.

Configuration The following example specifies the URL of the CPE to <http://10.10.10.1:7547/acs>.

Examples

```
Ruijie#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe url http://10.10.10.1:7547/
```

```
Ruijie(config-cwmp) #
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.8 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.

acs username *username*

No acs 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 Mode cwmp config 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.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe username admin
Ruijie(config-cwmp) #
```

Related Commands

Command	Description
show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.
cpe password	Configures the CPE password to be

	authenticated for the ACS to connect to the CPE.
--	--------------------------------------------------

Platform N/A
Description

9.9 cwmp

Use this command to enable the CWMP function.
 Use the **no** form of this command to disable this function.

cwmp
no cwmp

Parameter Description	Parameter	Description
	N/A	N/A

Defaults N/A

Command Mode Global configuration mode

Usage Guide Use this command to enable or disable the CWMP function.

Configuration The following example disables the CWMP function.

```
Examples
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#no cwmp
Ruijie(config)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
show cwmp status	Displays the running status of CWMP.	

Platform N/A
Description

9.10 disable download

Use this command to disable the function of downloading main program and configuration files from the ACS. Use the **no** form of this command to restore the default setting.

disable download

no disable download

Parameter Description	Parameter	Description
		N/A

Defaults By default, the CPE can download main program and configuration files from the ACS.

Command Mode CWMP configuration mode

Usage Guide N/A

Configuration Examples The following example disables the function of downloading main program and configuration files from the ACS.

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable download
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform Description N/A

9.11 disable upload

Use this command to disable the function of uploading configuration and log files 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

Defaults By default, the CPE can upload its configuration and log files to the ACS.

Command Mode CWMP configuration mode

Usage Guide Disables the function of uploading configuration and log files to the ACS.

Configuration The following example disables the function of uploading configuration and log file to the ACS.

```
Examples
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable upload
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform N/A

Description

9.12 disable stun

Use this command to disable STUN port adaptation. Use the **no** form of this command to enable STUN port adaptation.

- disable stun port-adaptive**
- no disable stun port-adaptive**

Parameter Description	Parameter	Description
		port-adaptive

Defaults STUN port adaptation is disabled by default.

Command Mode CWMP configuration mode

Usage Guide Use this command to enable STUN port adaptation.

Configuration Examples The following example enables STUN port adaptation. The device will adapt to STUN server port 3478 and 3479.

```

Hostname> enable
Hostname# configure terminal
Hostname(config)# cwmp
Hostname(config-cwmp)# no disable stun port-adaptive
Hostname(config-cwmp)#
```

Related Commands	Command	Description
		N/A

Platform N/A
Description

9.13 show cwmp configuration

Use this command to display the current configuration of CWMP.

show cwmp configuration

Parameter Description	Parameter	Description
		N/A

Defaults N/A

Command Mode Privilege EXEC mode

Usage Guide N/A

Configuration Examples The following example displays the current configuration of CWMP.

```
Ruijie(config-cwmp)#show cwmp configuration
CWMP Status           : enable
ACS URL                : http://www.ruijie.com.cn/acs
ACS username          : admin
ACS password           : *****
CPE URL                : http://10.10.10.2:7547/
CPE username          : ruijie
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
CPE STUN port-adaptive : disable
CPE STUN port         : 3478
CPE STUN max-period   : 60s
CPE STUN min-period   : 20s
```

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	Indicates whether to upload configuration files and log files 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.
CPE STUN port-adaptive	Indicates whether to enable STUN port adaptation.
CPE STUN port	Indicates the STUN server port.
CPE STUN max-period	Indicates the max STUN keepalive interval.
CPE STUN min-period	Indicates the min STUN keepalive interval.

Related Commands

Command	Description
show cwmp status	Displays the running status of CWMP.

Platform N/A
Description

9.14 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 Ruijie#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
    
```

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
	show cwmp configuration	Displays the current configuration of CWMP.

Platform Description N/A

9.15 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>	Sets the session timeout, in the range from 10 to 600 in the unit of seconds.

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 The following example configures the session timeout period of the CPE to 50 seconds.

Examples

```
Ruijie#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#timer cpe-timeout 50
Ruijie(config-cwmp)#
```

Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform Description N/A

10 PoE Management Commands

10.1 poe class-lldp enable

Use this command to configure LLDP two-event classification. Use the **no** or **default** form of this command to restore the default setting.

poe class-lldp enable

no poe class-lldp enable

default poe class-lldp enable

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example enables LLDP two-event classification.

```
Ruijie(config)# poe class-lldp enable
Ruijie(config)# end
Ruijie#write
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

10.2 poe enable

Use this command to enable the power over Ethernet (PoE) function on the interface. Use the **no** form of this command to disable this function.

poe enable

no poe enable

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

Description		
	N/A	N/A

Defaults This function is enabled by default,

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example disables the PoE function on port GigabitEthernet 0/1,

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no poe enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.3 poe legacy

Use this command to enable non-standard PD compatibility. Use the **no** or **default** form of this command to restore the default setting.

poe legacy

no poe legacy

default poe legacy

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 enables non-standard compatibility for port GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe legacy
```


Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.4 poe max-power

Use this command to set the maximum power for the port. Use the **no** or **default** form of this command to restore the default setting,

poe max-power *int*
no poe max-power
default poe max-power

Parameter Description	Parameter	Description
	<i>int</i>	The maximum power, in the range from 0 to 30W. Note that this parameter is in the range from 0 to 15.4W on the system supporting 802.3af only. HPoE port ID is in the range from 0 to 90.

Defaults The maximum power is not set by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the maximum power for port GigabitEthernet 0/1 to 20W.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe max-power 20
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.5 poe mode

Use this command to set the PoE management mode. Use the **no** or **default** form of this command to restore the default setting.

poe mode { auto | energy-saving }

no poe mode

default poe mode

Parameter Description	Parameter	Description
	auto	Sets the power management mode to auto mode, the default mode.
	energy-saving	Sets the power management mode to energy-saving mode, the optional mode,

Defaults The default mode is auto.

Command Mode Global configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PoE management mode to energy-saving mode.

```
Ruijie# configure
Ruijie(config)# poe mode energy-saving
Ruijie(config)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.6 poe notification-control enable

Use this command to enable Trap notification in PoE MIB(RFC3621). Use the **no** or **default** form of this command to restore the default setting.

poe notification-control enable

no poe notification-control enable

default poe notification-control enable

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

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

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables Trap notification in PoE MIB(RFC3621).

Examples

```
Ruijie(config)# poe notification-control enable
Ruijie(config)# end
Ruijie#write
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.7 poe pd-description

Use this command to set the PD descriptor for the port. Use the **no** or **default** form of this command to restore the default setting.

- poe pd-description** *pd-name*
- no poe pd-description**
- default poe pd-description**

Parameter Description	Parameter	Description
	<i>pd-name</i>	

Defaults N/A

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example sets the PD descriptor for port GigabitEthernet 0/1.

Examples

```
Ruijie# configure
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe pd-description ap220
```

```
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

10.8 poe power-off time-range name

Use this command to configure scheduled power-on for the port. Use the **no** or **default** form of this command to restore the default setting.

poe power-off time-range *name*

no poe power-off time-range

default poe power-off time-range

**Parameter
Description**

Parameter	Description
<i>name</i>	Time-range name.

Defaults

N/A

**Command
Mode**

Interface configuration mode

Usage Guide

N/A

Configuration The following example sets the port GigabitEthernet 0/1 to be disabled from 8:30 to 17:30 every day.

Examples

```
Ruijie# configure
Ruijie(config)# time-range poe-time
Ruijie(config-time-range)# periodic weekdays 8:30 to 17:30
Ruijie(config-time-range)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe power-off time-range poe-time
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

10.9 poe priority

Use this command to set the PoE priority for the port. Use the **no** or **default** form of this command to restore the default setting.

poe priority { low | high | critical }

no poe priority

default poe priority

Parameter Description	Parameter	Description
	{ low high critical }	Priority level.

Defaults The default is low.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example sets the PoE priority for port GigabitEthernet 0/1 to critical.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# poe priority critical
Ruijie(config-if-GigabitEthernet 0/1)# end
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

10.10 poe uninterruptible-power

Use this command to configure uninterruptible warm start, Use the **no** or **default** form of this command to restore the default setting.

poe uninterruptible-power

no poe uninterruptible-power

default no poe uninterruptible-power

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function takes effect when the device is started after the configuration is saved.

Configuration The following example enables uninterruptible PoE for warm start and saves configuration.

```
Ruijie(config)# poe uninterruptible-power
Ruijie(config)# end
Ruijie#write
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

10.11 poe warning-power

Use this command to set the power alarm threshold for the system. Use the **no** or **default** form of this command to restore the default setting,

```
poe warning-power int
no poe warning-power
default poe warning-power
```

Parameter Description

Parameter	Description
<i>int</i>	Power alarm threshold (percentage), in the range from 0 to 99.

Defaults The default is 99.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example sets the power alarm threshold for the system to 80%.

```
Ruijie(config)# poe warning-power 80
Ruijie(config)# end
Ruijie#write
```

Related

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

Commands		
	N/A	N/A

Platform N/A

Description

10.12 poe auto-checking pd-address

Use this command to configure the IP of PD device. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking pd-address *ip-address interface interface-type interface-number*

no poe auto-checking pd-address *ip-address interface interface-type interface-number*

default poe auto-checking pd-address *ip-address interface interface-type interface-number*

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>interface-type</i>	Specifies the interface type.
	<i>interface-number</i>	Specifies the interface number.

Defaults N/A

Command Interface configuration mode

Mode

Usage Guide N/A

Configuration The following example adds 192.168.21.139 as the auto-checking PD device.

Examples

```
Ruijie(config-if-VLAN 1)#poe auto-checking pd-address 192.168.21.139
interface gigabitEthernet 0/1
```

Related Commands	Command	Description
	show poe auto-checking	Displays the PoE auto-checking configuration.

Platform N/A

Description

10.13 poe auto-checking interval-time

Use this command to configure the detection interval of PoE auto-checking. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking interval-time *interval*
no poe auto-checking interval-time
default poe auto-checking interval-time

Parameter Description	Parameter	Description
	<i>interval</i>	The detection interval of PoE auto-checking, in the range from 10 to 120.

Defaults The detection interval is 10 seconds by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures the detection interval of PoE auto-checking.

```
Ruijie(config-if-VLAN 1)#poe auto-checking interval-time 60
```

Related Commands	Command	Description
	show poe auto-checking	Displays the PoE auto-checking configuration.

Platform Description N/A

10.14 poe auto-checking retry-time

Use this command to configure the retry times for one PoE auto-checking. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking retry-time *int*
no poe auto-checking retry-time
default poe auto-checking retry-time

Parameter Description	Parameter	Description
	<i>int</i>	Detection retry times, in the range from 1 to 5.

Defaults The default is 1.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example configures the detection retry times of PoE auto-checking.

Examples

```
Ruijie(config-if-VLAN 1)#poe auto-checking retry-time 2
```

Related Commands	Command	Description
		show poe auto-checking

Platform N/A

Description

10.15 poe auto-checking failure-action

Use this command to configure the action after detecting that the PD is offline. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking failure-action [nothing | reboot-remote-pd]

no poe auto-checking failure-action

default poe auto-checking failure-action

Parameter Description	Parameter	Description
		[nothing reboot-remote-pd]

Defaults It is configured as **nothing** by default.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration The following example configures the PD offline action of PoE auto-checking.

Examples

```
Ruijie(config-if-VLAN 1)#poe auto-checking failure-action reboot-remote-pd
```

Related Commands	Command	Description
		show poe auto-checking

Platform N/A

Description

10.16 poe auto-checking reboot-time

Use this command to configure the reboot waiting time of PoE auto-checking. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking reboot-time *interval*

no poe auto-checking reboot-time

default poe auto-checking reboot-time

Parameter Description	Parameter	Description
	<i>interval</i>	The reboot waiting time of PoE auto-checking, in the range from 10 to 120.

Defaults The default is 15 seconds.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples The following example configures the reboot waiting time of PoE auto-checking.

```
Ruijie(config-if-VLAN 1)#poe auto-checking reboot-time 30
```

Related Commands	Command	Description
	show poe auto-checking	Displays the PoE auto-checking configuration.

Platform Description N/A

10.17 poe auto-checking

Use this command to enable PoE auto-checking. Use the **no** or **default** form of this command to restore the default setting,

poe auto-checking

no poe auto-checking

default poe auto-checking

Parameter Description	Parameter	Description
	N/A	N/A

Defaults The function is disable by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables PoE auto-checking.

Examples `Ruijie(config)#poe auto-checking`

Related Commands	Command	Description
		show poe auto-checking status

Platform N/A

Description

10.18 show poe interface

Use this command to display PoE configuration and status of the specified port.

show poe interface *interface-name*

Parameter Description	Parameter	Description
		<i>interface-name</i>

Defaults N/A

Command Mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays the PoE configuration and status in interface GigabitEthernet 0/1.

Examples

```
Ruijie#show poe interface GigabitEthernet 0/1
Interface           : Gi0/1
Power enabled       : enable
Power status        : on
Max power           : N/A
Allocate power      : N/A
Current power       : 14.8 W
Average power       : 14.8 W
Peak power          : 14.8 W
Voltage             : 53.5 V
Current             : 278 mA
```

```

PD class           : 4
Trouble cause      : None
Priority           : critical
Legacy            : off
Power-off time-range : N/A
Power management   : auto
    
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

10.19 show poe interfaces

Use this command to display PoE status or configuration of all ports.

- show poe interfaces status**
- show poe interfaces configuration**

Parameter Description	Parameter	Description
	status	
configuration		Displays PoE configuration of all ports.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide This command is used to display PoE status or configuration of all ports.

Configuration Examples The following example displays PoE status of all ports.

```

Ruijie#show poe interfaces status
Interface Power   Power   Curr  Avg   Peak  Curr   Trouble PD   Port
          Control Status  Power Power Power Current Cause  Class Voltage
-----
Gi0/1    enable  on     14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/2    enable  on     28.4W 28.4W 28.4W 531mA  0     4    53.5V
Gi0/3    enable  on     14.9W 14.9W 14.9W 279mA  0     4    53.5V
Gi0/4    enable  off    0.0W  0.0W  0.0W  0mA   6     N/A  0.0V
Gi0/5    enable  on     14.8W 14.8W 14.8W 278mA  0     4    53.5V
Gi0/6    enable  on     15.0W 15.0W 15.0W 281mA  0     4    53.5V
Gi0/7    enable  on     6.1W  6.1W  6.1W  115mA  0     4    53.5V
    
```

Gi0/8	enable	on	14.8W	14.8W	14.8W	277mA	0	4	53.5V
Gi0/9	enable	on	14.7W	14.7W	14.7W	276mA	0	4	53.5V
Gi0/10	enable	on	14.8W	14.8W	14.8W	278mA	0	4	53.5V
Gi0/11	enable	on	14.7W	14.7W	14.7W	275mA	0	4	53.5V
Gi0/12	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/13	enable	on	14.8W	14.8W	14.8W	278mA	0	4	53.5V
Gi0/14	enable	on	0.3W	0.3W	0.3W	7mA	0	4	53.5V
Gi0/15	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/16	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/17	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/18	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/19	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/20	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/21	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/22	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/23	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V
Gi0/24	enable	off	0.0W	0.0W	0.0W	0mA	6	N/A	0.0V

The following example displays PoE configuration of all ports.

```
Ruijie#show poe interfaces configuration
```

Interface	Power Control	Power Status	Max Power	Alloc Power	Port Priority	Port Legacy	Power-off Time-range
Gi0/1	enable	on	N/A	N/A	critical	off	N/A
Gi0/2	enable	on	N/A	N/A	critical	off	N/A
Gi0/3	enable	on	N/A	N/A	critical	off	N/A
Gi0/4	enable	off	N/A	N/A	critical	off	N/A
Gi0/5	enable	on	N/A	N/A	critical	off	N/A
Gi0/6	enable	on	N/A	N/A	high	off	N/A
Gi0/7	enable	on	N/A	N/A	high	off	N/A
Gi0/8	enable	on	N/A	N/A	high	off	N/A
Gi0/9	enable	on	N/A	N/A	high	off	N/A
Gi0/10	enable	on	N/A	N/A	high	off	N/A
Gi0/11	enable	on	N/A	N/A	high	off	N/A
Gi0/12	enable	off	N/A	N/A	high	off	N/A
Gi0/13	enable	on	N/A	N/A	low	off	N/A
Gi0/14	enable	on	N/A	N/A	low	off	N/A
Gi0/15	enable	off	N/A	N/A	low	off	N/A
Gi0/16	enable	off	N/A	N/A	low	off	N/A
Gi0/17	enable	off	N/A	N/A	low	off	N/A
Gi0/18	enable	off	N/A	N/A	low	off	N/A
Gi0/19	enable	off	N/A	N/A	low	off	N/A
Gi0/20	enable	off	N/A	N/A	low	off	N/A
Gi0/21	enable	off	N/A	N/A	low	off	N/A

Gi0/22	enable	off	N/A	N/A	low	off	N/A
Gi0/23	enable	off	N/A	N/A	low	off	N/A
Gi0/24	enable	off	N/A	N/A	low	off	N/A

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

10.20 show poe powersupply

Use this command to display the PoE power supply status.

show poe powersupply

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 PoE power supply status.

```
Ruijie#show poe powersupply
Device member           : 1
Power management        : auto
PSE total power         : 1000W
PSE total power consumption : 300W
PSE total remain power  : 700W
PSE total powered port  : 0
PSE disconnect mode     : dc
PSE reserve power       : 0%
PSE warning power       : 99%
PSE class lldp          : disable
PSE uninterruptible-power : disable
    PSE member           : 1
    PSE Power status     : normal
    PSE Power Enabled    : enable
    PSE max power        : 300W
```

```
PSE priority                : low
PSE alloc power             : 300W
PSE available power        : 300W
PSE total power consumption : 0 W
PSE total remain power     : 300W
PSE peak power             : 0 W
PSE average power          : 0 W
PSE powered port           : 0
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

10.21 show poe auto-checking

Use this command to display the PoE auto-checking configuration.

show poe auto-checking

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 PoE power supply status.

```
Ruijie# show poe auto-checking
PD device: 192.168.21.139, interfaces: VLAN 1, port: GigabitEthernet 0/1, check
interval: 10, retry time: 1, reboot_time: 15, fail action: nothing.
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

10.22 show poe auto-checking status

Use this command to display the PoE auto-checking status.

show poe auto-checking 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 PoE power supply status.

Examples

```
Ruijie# show poe auto-checking status
PD device: 192.168.21.139, fail_time: 0, total: 0, status: over.
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

Ethernet Configuration Commands

1. Interface Commands
2. MAC Address Commands
3. Aggregate Port Commands
4. VLAN Commands
5. MAC VLAN Commands
6. Protocol VLAN Commands
7. Private VLAN Commands
8. Voice VLAN Commands
9. VLAN Mapping Commands
10. STP/RSTP/MSTP Commands
11. LLDP Commands

1 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 unit of Kbps. The range is from 1 to 2147483647.

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.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# bandwidth 64
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

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 { [**milliseconds**] *num* | **up** [**milliseconds**] *num* }

no carrier-delay

Parameter Description	Parameter	Description
	<i>num</i>	(Optional) in the range from 0 to 60 in the unit of seconds.
	milliseconds	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
	up	(Optional) Configures the delay after which DCD changes from Down to Up in status.

Defaults The default is 2 seconds.

Command Mode Interface configuration mode

Usage Guide This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status. 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.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config)# carrier-delay 5
```

The following example sets the carrier delay of serial interface to 100 milliseconds.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# carrier-delay milliseconds 100
```

The following example sets the DCD delay from Down to Up in status to 100 milliseconds.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# carrier-delay up milliseconds 100
```

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</i> <i>interface-number</i>	Interface type and interface ID
--------------------------------------------------	---------------------------------

Defaults N/A

Command Mode Privileged EXEC 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 Examples The following example clears the counters on interface gigabitethernet 0/1.

```
Ruijie# clear counters gigabitethernet 0/1
```

Related Commands

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.4 clear interface

Use this command to reset the interface.

clear interface *interface-type interface-number*

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface type and interface ID

Defaults N/A

Command Mode Privileged EXEC 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 Examples The following example resets the interface gigabitethernet 0/1.

```
Ruijie# clear interface gigabitethernet 0/1
```

Related Commands	Command	Description
	shutdown	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

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 The following example configures the alias of interface.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# description GBIC-1
```

Related Commands	Command	Description
	show interfaces show interfaces description	Displays the interface alias.

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
	auto	Self-adaptive full duplex and half duplex
	full	Full duplex
	half	Half duplex

Defaults The default is **auto**,

Command Mode Interface configuration mode.

Usage Guide The duplex mode is associated with the interface type. Use **show interfaces** to display the duplex mode of the interface

Configuration Examples The following example specifies the duplex mode for the interface.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# duplex full
```

Related Commands	Command	Description
	show interfaces	Displays the interface information.

Platform Description N/A

1.7 eee enable

Use this command to enable Energy Efficient Ethernet (EEE) on the interface.

eee enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide Use this command to achieve EEE on the interface in Low Power Idle(LPI) mode,

Configuration Examples The following example enables EEE on GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# eee enable
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

1.8 errdisable recovery

Use this command to recover the interface in violation.

errdisable recovery [interval time]

**Parameter
Description**

Parameter	Description
interval time	Time for the command to take effect. The range is from 30 to 86,400 seconds.

Defaults By default, it is disabled.

**Command
Mode** Global configuration mode.

Usage Guide Use the **show interfaces status err-disable** command to recover the port that triggers violation after being configured with the **violation shutdown** command.

Configuration The following example recovers the violation interface.

Examples

```
Ruijie(config)# errdisable recovery
Ruijie(config)# end
```

**Related
Commands**

Command	Description
show interfaces status err-disable	Displays the interface violation information.

Platform N/A.
Description

1.9 flowcontrol

Use this command to enable or disable the flow control. Use the **no** form of this command to restore the default setting.

flowcontrol { auto | off | on }

no flowcontrol**Parameter
Description**

Parameter	Description
auto	Self-negotiates the flow control.
off	Disables the flow control.
on	Enables the flow control.

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide NA

Configuration Examples The following example enables flow control on gigabitethernet port 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# flowcontrol on
```

**Related
Commands**

Command	Description
show interfaces	Displays the interface information.

Platform Description N/A

1.10 interface

Use 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>	The interface ID.

Defaults N/A

Command Mode Global configuration mode

Usage Guide This command is used to enter interface configuration mode. The user can modify the interface configuration next,

Configuration The following example enters configuration mode on Aggregateport 1.

Examples

```
Ruijie(config)# interface Aggregateport 1
Ruijie(config-if-Aggregateport 1)#
```

The following example enters configuration mode on GigabitEthernet 0/2.

```
Ruijie(config)# interface Gigabitethernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)#
```

The following example configuration mode on VLAN 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)#
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

1.11 interface range

Use this command to enter interface configuration mode on multiple 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.
macro <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 enters interface configuration mode on multiple interfaces by setting the interface range.

```
Ruijie(config)# interface range gigabitethernet 0/1, 0/2
```

```
Ruijie(config-if-range)# bandwidth 100
```

The following example enters interface configuration mode on multiple interfaces by defining the macro name.

```
Ruijie(config)# define interface-range routel gigabitethernet 0/1-2
Ruijie(config)# interface range macro routel
Ruijie(config-if-range)# bandwidth 100
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.12 line-detect

Use this command to detect the cable connection status.

line-detect

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command Mode Interface configuration mode.

Usage Guide This command is used to detect the line status and locate the problem in case of a line failure, for example, the line is torn down.

Configuration Examples The following example detects the cable connection status on gigabitethernet 0/1.

```
Ruijie(config-if-GigabitEthernet 0/1)# line-detect
This operation may force the port down and up once, continue?[Y/N]:y
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs, length +/- 10 meters
pair state      length(meters)
-----
A   OK          4
B   OK          9
C   Short       4
D   Short       4
```

Field	Description
pairs	Number of line pairs included. For example, the twisted pair includes four pairs of lines.
state	Status of the current line pair: OK, Short or Open. In general, the 100M twisted pairs A and B are OK, C and D are Short. The 1000M twisted pairs A, B, C and D are all OK.
length	Length of the line in meter. Only the length of the line pair whose status is OK takes effect. Since the length is calculated based on the transmission time of signal, there may have a certain difference. The length of the line pair whose status is Short or Open is the length from the port to the faulty point.

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

1.13 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 The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180

Examples

seconds.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# load-interval 180
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

1.14 logging

Use this command to print information on the interface.

logging [**link-updown** | **error-frame** | **link-dither**]

**Parameter
Description**

Parameter	Description
link-updown	Prints the status change information.
error-frame	Prints the error frame information.
link-dither	Prints the oscillation information.

Defaults

This function is enabled by default.

**Command
Mode**

Global configuration mode

Usage Guide

N/A

Configuration

The following example prints information on the interface.

Examples

```
Ruijie(config)# logging link-updown
Ruijie(config)# logging error-frame
Ruijie(config)# logging link-dither
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

1.15 negotiation mode

Use this command to enable or disable auto-negotiation mode. Use the **no** form of this command to restore the default setting.

negotiation mode { on | off }

no negotiation mode

Parameter Description	Parameter	Description
	on	Enables auto-negotiation.
	off	Disables auto-negotiation.

Defaults This function is disabled by default.

Command Mode Interface configuration mode

Usage Guide In general, the auto-negotiation status is determined by interface speed, duplex, flow control and auto-negotiation factor mode.

Configuration Examples The following example enables auto-negotiation mode on interface GigabitEthernet 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# negotiation mode on
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.16 physical-port dither protect

Use this command to enable oscillation protection on the port.

physical-port dither protect


Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is enabled by default.

Command Global configuration mode

Mode

Usage Guide After you configure the **physical-port dither protect** command, the port will be shut down when the oscillation occurs for certain times.

 If oscillation 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 oscillation 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 oscillation protection on the port.

Examples

```
Ruijie(config)# physical-port dither protect
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

1.17 shutdown

Use this command to disable an interface. Use the **no** form of this command to enable a disabled port.


shutdown
no shutdown

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, the administrative status of an interface is Up.

Command Interface configuration mode
Mode

Usage Guide Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the **no shutdown** command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the **show interfaces** command.

 If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal.

Configuration The following example disables an interface.

Examples

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if-AggregatePort 1)# shutdown
```

The following example enables an interface.

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if-AggregatePort 1)# no shutdown
```

Related Commands

Command	Description
clear interface	Resets the hardware.
show interfaces	Displays the interface information.

Platform N/A

Description

1.18 snmp trap link-status

Use this command to send LinkTrap on a port. Use the **no** form of this command to disable this function.

snmp trap link-status

no snmp trap link-status

Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default

Command Mode Interface configuration mode.

Usage Guide For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.

Configuration Examples The following example disables the interface from sending LinkTrap on the interface.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

The following example enables the interface to forward Link trap.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# snmp trap link-status
```

Related Commands

Command	Description
snmp trap link-status	Enables the interface to send LinkTrap on the

	interface.
no snmp trap link-status	Disables the interface from sending LinkTrap on the interface.

Platform N/A

Description

1.19 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

```
Ruijie(config)# snmp-server if-index persist
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

1.20 speed

Use this command to configure the speed on the port. Use the **no** form of this command to restore the default setting.

speed [10 | 100 | 1000 | auto]

no speed

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

Description	
10	The transmission rate of the interface is 10Mbps.
100	The transmission rate of the interface is 100Mbps.
1000	The transmission rate of the interface is 1000Mbps.
auto	Self-adaptive

Defaults The default is **auto**.

Command Mode Interface configuration mode.

Usage Guide If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use **show interfaces** to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M or 100M.

Configuration The following example sets the speed on interface gigabitethernet 0/1 to 100Mbps.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# speed 100
```

Related Commands	Command	Description
	show interfaces	Displays the interface information.

Platform N/A

Description

1.21 switchport access

Use this command to configure an interface as a statics access port and add it to a VLAN. Use the **no** form of this command to restore the default setting.

switchport access vlan *vlan-id*

no switchport access vlan

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN ID at which the port to be added.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command Mode Interface configuration mode.

Usage Guide Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN. If the port is a trunk port, the operation does not take effect.

Configuration Examples The following example configures interface gigabitethernet 0/1 as a statistic access port and adds it to VLAN 2.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

Related Commands

Command	Description
switchport mode	Configures the interface as Layer 2 mode (switch port mode).
switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunkport.

Platform N/A

Description

1.22 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the **no** form of this command to restore the default setting.

switchport mode { access | trunk }

no switchport mode

Parameter Description

Parameter	Description
access	Configures the switch port as an access port.
trunk	Configures the switch port as a trunk port.

Defaults The default is **Access**.

Command Mode Interface configuration mode.

Usage Guide If a switch port mode is access port, it can be the member port of only one VLAN. Use **switchport access vlan** to specify the member of the VLAN.

A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use **switchport trunk** to define the allowed-VLANs list.

Configuration The following example specifies a L2 interface (switch port) mode.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

Related Commands	Command	Description
	switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
	switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunk port.

Platform N/A

Description

1.23 switchport trunk

Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the **no** form of this command to restore the default setting.

switchport trunk { allowed vlan { all | [add | remove | except] *vlan-list* } | native vlan *vlan-id* }

no switchport trunk { allowed vlan | native vlan }

Parameter Description	Parameter	Description
	allowed vlan <i>vlan-list</i>	Configures the list of VLANs allowed on the trunk port. <i>vlan-list</i> can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
	native vlan <i>vlan-id</i>	Configures the native VLAN. The range is from 1 to 4094.

Defaults The allowed VLAN list is all, the Native VLAN is VLAN1.

Command Interface configuration mode.

Mode

Usage Guide Native VLAN:

A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged.

Allowed-VLAN List:

By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk. Use `show interfaces switchport` to display configuration.

Configuration The following example configures the native VLAN of GigabitEthernet 0/1 as VLAN 2 .

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport trunk native vlan 2
```

Related Commands

Command	Description
<code>show interfaces</code>	Displays the interface information.
<code>Switchport access</code>	Configures an interface as a statics access port and assigns it to a VLAN.

Platform N/A

Description

1.24 show eee interfaces status

Use this command to display interface EEE status.

`show eee interfaces { interface-type interface-number | status }`

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	Interface type and ID.
<i>Status</i>	All interface EEE status.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If the interface is specified, the EEE status of the specified interface is displayed; otherwise, the EEE status of all interfaces is displayed.

Configuration Examples The following example displays EEE status of interface GigabitEthernet 0/1.

```
Ruijie# show eee interface gigabitethernet 0/1
```

```
Interface          : Gi0/1
EEE Support        : Yes
Admin Status      : Enable
Oper Status       : Disable
Remote Status     : Disable
Trouble Cause     : Remote Disable
```

Field	Description
EEE Support	Whether EEE is supported
Admin Status	Configuration status
Oper Status	Operation status
Trouble Cause	Trouble cause

The following example displays EEE status of all interfaces.

```
Ruijie# show eee interface status
Interface EEE      Admin   Oper   Remote  Trouble
           Support Status   Status Status   Cause
-----
Gi0/1   Yes   Enable  Disable  Disable  Remote Disable
Gi0/2   Yes   Enable  Disable  Unknown  None
Gi0/3   Yes   Enable  Enable   Enable   None
Gi0/4   Yes   Enable  Enable   Enable   None
Gi0/5   Yes   Enable  Enable   Enable   None
Gi0/6   Yes   Enable  Enable   Enable   None
Gi0/7   Yes   Enable  Enable   Enable   None
Gi0/8   Yes   Enable  Enable   Enable   None
Gi0/9   Yes   Enable  Enable   Enable   None
Gi0/10  Yes   Enable  Enable   Enable   None
Gi0/11  Yes   Enable  Enable   Enable   None
Gi0/12  Yes   Enable  Enable   Enable   None
Gi0/13  Yes   Enable  Enable   Enable   None
Gi0/14  Yes   Enable  Enable   Enable   None
Gi0/15  Yes   Enable  Enable   Enable   None
Gi0/16  Yes   Enable  Enable   Enable   None
Gi0/17  Yes   Enable  Enable   Enable   None
Gi0/18  Yes   Enable  Enable   Enable   None
Gi0/19  Yes   Enable  Enable   Enable   None
Gi0/20  Yes   Enable  Enable   Enable   None
Gi0/21  Yes   Enable  Enable   Enable   None
Gi0/22  Yes   Enable  Enable   Enable   None
Gi0/23  Yes   Enable  Enable   Enable   None
Gi0/24  Yes   Enable  Enable   Enable   None
Gi0/25  No    -      -      -        -
Gi0/26  No    -      -      -        -
Gi0/27  No    -      -      -        -
```

Gi0/28 No - - - -

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.25 show interfaces

Use this command to display the interface information and optical module information.

show interfaces [*interface-type interface-number*] [**description** | **switchport**]

Parameter Description

Parameter	Description
<i>interface-type interface-number</i>	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
description	The description of the interface, including the link status.
switchport	Layer 2 interface information.

Defaults

Command Mode Privileged EXEC mode.

Usage Guide This command is used to show all basic information if no parameter is specified.

Configuration Examples The following example displays the interface information when the Gi0/1 is a Trunk port.

```
Ruijie# 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
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
RXload is 1 ,Txload is 1
Queueing strategy: FIFO
Output queue 0/1, 0 drops;
Input queue 0/75, 0 drops
Switchport attributes:
interface's description:""
```

```

medium-type is copper
lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
Priority is 0
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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: trunk
Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
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 the interface information when the Gi0/1 is an Access port.

```

Ruijie# 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
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
RXload is 1 ,Txload is 1
Queueing strategy: FIFO
Output queue 0/0, 0 drops;
Input queue 0/75, 0 drops
Switchport attributes:
interface's description:""
medium-type is copper
lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
Priority is 0
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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: access
Vlan id : 2
  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 the layer-2 interface information when the Gi0/1 is a Hybrid port.

```

Ruijie# 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
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    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
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control
is OFF
Port-type: hybrid
Tagged vlan id:2
Untagged vlan id:none
  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 the layer-2 information of the Gi0/1.

```

Ruijie# show interfaces gigabitethernet 0/1 switchport
Interface Switchport ModeAccess Native Protected VLAN lists
-----
GigabitEthernet 0/1 enabled Access 11 Disabled ALL
    
```

Related Commands

Command	Description
duplex	Duplex
flowcontrol	Flow control status.
interface gigabitethernet	Selects the interface and enter the interface configuration mode.
interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
shutdown	Disables the interface.
speed	Configures the speed on the port.
switchport priority	Configures the default 802.1q interface priority.
switchport protected	Configures the interface as a protected port.

Platform N/A

Description

1.26 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**]

Parameter Description	Parameter	Description
	<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.
	increment	Displays the packet statistics increased during the last sample interval.
	error	Displays error packet statistics.
	rate	Displays packet receiving and transmitting rate.

summary	Displays packet statistics summary.
----------------	-------------------------------------

Defaults N/A

Command Mode Any CLI 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

```
Ruijie# 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.

```

Ruijie# 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.

```

Ruijie# 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 is the number of valid packets smaller than 64 bytes.
 OverSize is the number of valid packets smaller than 1518 bytes.
 Collisions is the number of colliding transmit packets.
 Fragments is the number of packets with CRC error or frame alignment error which are smaller

than 64 bytes.

Jabbers is the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.

CRC-Align-Err is the number of receive packets with CRC error.

Align_Err is the number of receive packets with frame alignment error.

FCS-Err is the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on interface GigabitEthernet 0/1.

```
Ruijie# 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
```

i 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 interface GigabitEthernet 0/1.

```
Ruijie# 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
```

i 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.

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

1.27 show interfaces link-state-change statistics

Use this command to display the link state change statistics, including the time and count.

show interfaces [*interface-type interface-number*] **link-state-change statistics**

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type and ID.
	<i>interface-number</i>	

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the link state statistics of all interfaces are displayed.

Configuration Examples The following example displays the link state statistics of interface GigabitEthernet 0/1.

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface  Link state  Link state change times  Last change time
-----
Gi 0/1    down      100                      2012-12-24 15:00:00
```

Interface	Description
Link state	Current link state.
Link state change times	The count of link state change.
Last change time	The time when the last link state change occurs.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

1.28 show interfaces status

Use this command to display interface status information.

show interfaces [*interface-type interface-number*] **status**

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type and ID.
	<i>interface-number</i>	
	status	Displays interface status information, including speed and duplex.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide If you do not specify an interface, the status information of all interfaces is displayed.
If you specify an AP port, the **Speed** column in the output of this command displays the speed of each AP member port.

Configuration The following example displays the status information of interface GigabitEthernet 0/1.

Examples

```
Ruijie# show interfaces GigabitEthernet 0/1 status
Interface          Status      Vlan    Duplex  Speed  Type
-----
GigabitEthernet 0/1  up         1       Full   1000M  copper
```

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.29 show interfaces status err-disable

Use this command to display the interface violation status.

show interfaces [*interface-type interface-number*] **status err-disable**

Parameter Description

Parameter	Description
<i>interface-type</i> <i>interface-number</i>	(Optional) The interface type and ID.

Defaults

Command Mode Any CLI mode


Usage Guide If you do not specify an interface, violation status of all interfaces is displayed.

Configuration The following example displays the violation status of interface GigabitEthernet 0/1.

Examples

```
Ruijie# show interface gigabitethernet 0/1 status err-disabled
Interface          Status      Reason
-----
```

```
GigabitEthernet 0/1          err-disabled  BPDU Guard
```

 The violation status is displayed as **err-disabled**.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.30 show interfaces usage

Use this command to display bandwidth usage of the interface.

show interfaces [*interface-type interface-number*] **usage**

Parameter Description

Parameter	Description
<i>interface-type</i>	(Optional) The interface type and ID.
<i>interface-number</i>	


Defaults N/A

Command Mode Any CLI mode

Usage Guide If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the *bandwidth* parameter configured on the interface.

Configuration Examples The following example displays bandwidth usage of interface GigabitEthernet 0/1.

```
Interface          Bandwidth  Average Usage  Output Usage  Input Usage
-----
GigabitEthernet 0/1  1000 Mbit   0.002822759%  0.001183280%  0.004462237%
```

 Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.

Related Commands

Command	Description
N/A	N/A

Platform Description N/A

1.31 switchport protected

Use this command to configure the interface as the protected port. Use the **no** form of this command to restore the default setting.

switchport protected

no switchport protected

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guide The ports that are set as the protected ports cannot switch on L2, but can route on L3. A protected port can communicate with an unprotected port. Use the **show interfaces** command to display configuration.

Configuration Examples The following example configures interface `gigabitethernet 0/1` as a protected port.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport protected
```

Related Commands	Command	Description
	show interfaces	Displays the interface information.

Platform N/A

Description

2 MAC Address Commands

2.1 clear mac-address-table dynamic

Use this command to clear the dynamic MAC address.

```
clear mac-address-table dynamic [ address mac-address [ interface interface-id ] [ vlan vlan-id ] |
{ [ interface interface-id ] [ vlan vlan-id ] }
```

Parameter	Parameter	Description
Description	dynamic	Clears all the dynamic MAC addresses.
	address <i>mac-address</i>	Clears the specified dynamic MAC address.
	interface <i>interface-id</i>	Clears all the dynamic MAC addresses of the specified interface.
	vlan <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 Examples The following command clears all the dynamic MAC addresses.

```
Ruijie# clear mac-address-table dynamic
```

Related Commands	Command	Description
	show mac-address-table dynamic	Displays dynamic MAC address.

Platform Description N/A

2.2 mac-address-learning (global)

Use this command to enable MAC address learning globally. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning enable

Use this command to disable MAC address learning globally.

mac-address-learning disable

Use this command to restore MAC address learning globally.

default mac-address-learning

Parameter	Parameter	Description
Description	enable	Enables MAC address learning globally.
	disable	Disables MAC address learning globally.

Defaults The **mac-address-learning enable** command is enabled by default.

Command Mode Global configuration mode

Usage Guide When this function is enabled, the MAC address is learned in global configuration mode the same as learned in interface configuration mode.

Configuration Examples The following example disables MAC address learning globally.

```
Ruijie(config)# mac-address-learning disable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

2.3 mac-address-learning

Use this command to enable the port address learning. Use the **no** or **default** form of this command to restore the default setting.

mac-address-learning

no mac-address-learning

default mac-address-learning

Parameter	Parameter	Description
Description	N/A	N/A

Defaults The address learning function is enabled.

Command Mode Interface configuration mode.

Usage Guide MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.

Configuration The following example disables the port address learning function.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no mac-address-learning
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

2.4 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**

Parameter	Description
<i>seconds</i>	Aging time of the dynamic MAC address (in seconds). The time range is 0, 10-630.

Defaults The default is 300.

**Command
Mode** Global configuration mode.

Usage Guide Use **show mac-address-table aging-time** to display configuration.

Configuration The following example sets the aging time of the dynamic MAC address to 500 seconds.

Examples

```
Ruijie(config)# mac-address-table aging-time 500
```

**Related
Commands**

Command	Description
show mac-address-table aging-time	Displays the aging time of the dynamic MAC address.
show mac-address-table dynamic	Displays dynamic MAC address.

Platform N/A
Description

2.5 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*

Parameter	Parameter	Description
Description	<i>mac-address</i>	Filtering Address
	<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

Defaults No filtering address is configured by default.

Command Mode Global configuration mode.

Usage Guide The filtering MAC address shall not be a multicast address.

Configuration The following example configures the filtering MAC address for VLAN 3.

Examples

```
Ruijie(config)# mac-address-table filtering 0000.0202.0303 vlan 3
```

Related Commands	Command	Description
	clear mac-address-table filtering	Clears the filtering MAC address.

Platform Description N/A

2.6 mac-address-table notification

Use this command to enable the MAC address notification function. Use The **no** or **default** form of the command to restore the default setting.

mac-address-table notification [**interval** *value* | **history-size** *value*]

no mac-address-table notification [**interval** | **history-size**]

default mac-address-table notification [**interval** | **history-size**]

Parameter	Parameter	Description
Description	interval <i>value</i>	Sets the interval of sending the MAC address trap message, in the range from 1 to 3600, 1 second by default.
	history-size <i>value</i>	Sets the maximum number of the entries in the MAC address notification table, in the range from 1 to 200, 50 entries by default.

Defaults By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.

Command Mode Global configuration mode.

Usage Guide The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the **snmp-server enable traps mac-notification** command to enable or disable the switch to send the MAC address trap message.

Configuration The following example enables the MAC address notification function.

Examples

```
Ruijie(config)# mac-address-table notification
Ruijie(config)# mac-address-table notification interval 40
Ruijie(config)# mac-address-table notification history-size 100
```

**Related
Commands**

Command	Description
snmp-server enable traps	Sets the method of handling the MAC address trap message.
show mac-address-table notification	Displays the MAC address notification configuration and the MAC address trap notification table.
snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.

Platform N/A

Description

2.7 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-id*

no mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

default mac-address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**Parameter
Description**

Parameter	Description
<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-id</i>	Interface (physical interface or aggregate port) that packets are forwarded to

Defaults No static MAC address is configured by default.

Command Global configuration mode.

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 **show mac-address-table static** to display the static MAC address.

Configuration N/A

Examples

Related Commands	Command	Description
	<code>show mac-address-table static</code>	Displays the static MAC address.

Platform N/A

Description

2.8 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 All modes.

Mode

Usage Guide N/A

Configuration The following example displays the MAC address learning.

Examples

```
Ruijie# show mac-address-learning
GigabitEthernet 0/1    learning ability: disable
GigabitEthernet 0/2    learning ability: enable
GigabitEthernet 0/3    learning ability: enable
GigabitEthernet 0/4    learning ability: enable
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

2.9 show mac-address-table

Use this command to display all types of MAC addresses (including dynamic address, static address and filter address).

show mac-address-table [address *mac-addr*] [interface *interface-id*] [vlan *vlan-id*]

Parameter	Parameter	Description
Description	address <i>mac-addr</i>	The MAC address.
	interface <i>interface-id</i>	The Interface ID.
	vlan <i>vlan-id</i>	The VLAN ID, in the range from 1 to 4094.

Defaults N/A

Command Mode All modes

Usage Guide STATIC indicates static addresses, DYNAMIC indicates dynamic addresses, FILTER indicates filtering addresses, and OTHER indicates user addresses successfully authenticated.

Configuration The following example displays the MAC address.

Examples

```
Ruijie# show mac-address-table address 00d0.f800.1001
Vlan      MAC Address      Type      Interface
-----  -
1         00d0.f800.1001  STATIC   GigabitEthernet 0/1
Ruijie# 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 Description N/A

2.10 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
Description	N/A	N/A
Defaults	N/A	
Command Mode	All modes.	
Usage Guide	N/A	
Configuration	The following example displays the aging time of the dynamic MAC address.	
Examples	<pre>Ruijie# show mac-address-table aging-time Aging time : 300</pre>	
Related Commands	Command	Description
	mac-address-table aging-time	Sets the aging time of the dynamic MAC address.
Platform Description	N/A	

2.11 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-id* | **vlan** *vlan-id*]

Parameter	Parameter	Description
Description	interface <i>interface-id</i>	Interface ID
	vlan <i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	<p>The show mac-address-table count command is used to display the number of entries based on the type of MAC address entry.</p> <p>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.</p> <p>The show mac-address-table count vlan command is used to display the number of entries based on the VLAN of MAC address entries.</p>	
Configuration	The following example displays the number of MAC address entries.	
Examples	<pre>Ruijie# show mac-address-table count</pre>	


```
Dynamic Address Count : 51
Static Address Count : 0
Filter 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.

```
Ruijie# show mac-address-table count vlan 1
Dynamic Address Count : 7
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 7
```

The following example displays the number of MAC addresses on interface g0/1.

```
Ruijie# show mac-address-table interface gigabitethernet 0/1
Dynamic Address Count : 10
Static Address Count : 0
Filter Address Count : 0
Total Mac Addresses : 10
```

Related Commands

Command	Description
show mac-address-table static	Displays the static address.
show mac-address-table filtering	Displays the filtering address.
show mac-address-table dynamic	Displays the dynamic address.
show mac-address-table address	Displays all the address information of the specified address.
show mac-address-table interface	Displays all the address information of the specified interface.
show mac-address-table vlan	Displays all the address information of the specified vlan.

Platform N/A

Description

2.12 show mac-address-table dynamic

Use this command to display the dynamic MAC address.

```
show mac-address-table dynamic [ address mac-address ] [ interface interface-id ] [ 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-id</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**

```
Ruijie# show mac-address-table dynamic
Vlan  MAC Address      Type  Interface      Time
-----
1      0000.0000.0001     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:13:15
1      0001.960c.a740     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:13:16
1      0007.95c7.dff9     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:14:15
1      0007.95cf.eee0     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:15:20
1      0007.95cf.f41f     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:18:30
1      0009.b715.d400     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:20:55
1      0050.bade.63c4     DYNAMIC  gigabitethernet 0/1  2020-12-09 8:23:18
```

Related**Commands**

Command	Description
clear mac-address-table dynamic	Clears the dynamic MAC address.

Platform N/A**Description**

2.13 show mac-address-table filtering

Use this command to display the filtering MAC address.

show mac-address-table filtering [**addr** *mac-addr*] [**vlan** *vlan-id*]**Parameter****Description**

Parameter	Description
<i>mac-addr</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**

```
Ruijie# show mac-address-table filtering
Vlan  MAC Address      Type  Interface      Time
```

```
-----
1    0000.2222.2222  FILTER Not available          2020-12-09 9:16:33
```

Related Commands	Command	Description
	mac-address-table filtering	Configures the filtering MAC address.

Platform N/A

Description

2.14 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-id*] [**vlan** *vlan-id*]

Parameter	Parameter	Description
Description	<i>interface-id</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.

```
Ruijie# show mac-address-table interface
gigabitethernet 0/1
Vlan  MAC Address  Type   Interface          Time
-----
1     00d0.f800.1001  STATIC gigabitethernet 0/1  2020-12-09 13:11:33
1     00d0.f800.1002  STATIC gigabitethernet 0/1  2020-12-09 13:16:56
1     00d0.f800.1003  STATIC gigabitethernet 0/1  2020-12-09 14:18:14
1     00d0.f800.1004  STATIC gigabitethernet 0/1  2020-12-09 14:20:22
```

Related Commands	Command	Description
	show mac-address-table static	Displays the static MAC address.
	show mac-address-table filtering	Displays the filtering MAC address.
	show mac-address-table dynamic	Displays the dynamic MAC address.
	show mac-address-table address	Displays all types of MAC addresses.
	show mac-address-table vlan	Displays all types of MAC addresses of the specified VLAN.

show mac-address-table count	Displays the address counts in the MAC address table.
-------------------------------------	-------------------------------------------------------

Platform N/A

Description

2.15 show mac-address-table notification

Use this command to display the MAC address notification configuration and the MAC address notification table.

show mac-address-table notification [**interface** [*interface-id*] | **history**]

Parameter	Parameter	Description
Description	interface	Displays the MAC address notification configuration on all interfaces.
	interface <i>interface-id</i>	Displays the MAC address notification configuration on a specific interface.
	history	Displays the MAC address notification history.

Defaults

Command Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration The following example displays the MAC address notification configuration globally.

Examples

```
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

The following example displays the MAC address notification status.

```
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
Ruijie# show mac-address-table notification interface GigabitEthernet 0/2
Interface          MAC Added Trap    MAC Removed Trap
-----
GigabitEthernet 0/2  Enabled          Enabled
```

Related	Command	Description
Commands	mac-address-table notification	Enables MAC address notification.

snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.
-----------------------------------	--------------------------------------------------------------------------------

Platform N/A

Description

2.16 show mac-address-table static

Use this command to display the static MAC address.

show mac-address-table static [**addr** *mac-addr* *r*] [**interface** *interface-Id*] [**vlan** *vlan-id*]

Parameter	Parameter	Description
Description	<i>mac-addr</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-id</i>	Interface of the entry physical interface or aggregate port

Defaults N/A

Command Privileged EXEC mode.

Mode

Usage Guide N/A

Configuration The following example displays the static MAC addresses

Examples

```
Ruijie# show mac-address-table static
Vlan    MAC Address      Type    Interface          Time
-----
1 00d0.f800.1001  STATIC  gigabitethernet 0/1  2020-12-10 8:13:15
1 00d0.f800.1002  STATIC  gigabitethernet 0/1  2020-12-10 8:15:47
1 00d0.f800.1003  STATIC  gigabitethernet 0/1  2020-12-10 8:20:00
```

Related	Command	Description
Commands	mac-address-table static	Configures the static MAC address.

Platform N/A

Description

2.17 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
-----------	-----------	-------------

Description	<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

```
Ruijie# 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
	show mac-address-table static	Displays static addresses.
	show mac-address-table filtering	Displays filtered addresses.
	show mac-address-table dynamic	Displays dynamic addresses.
	show mac-address-table address	Displays all address information about the specified address.
	show mac-address-table interface	Displays all address information about the specified interface.
	show mac-address-table count	Displays the number of addresses in the address table.

Platform N/A
Description

2.18 snmp trap mac-notification

Use this command to enable the MAC address trap notification on the specified interface. Use The **no** or **default** form of the command to restore the default setting.

snmp trap mac-notification { added | removed }

no snmp trap mac-notification { added | removed }

default snmp trap mac-notification { added | removed }

Parameter	Parameter	Description
Description	<i>added</i>	Notifies when a MAC address is added.
	<i>removed</i>	Notifies when a MAC address is removed

Defaults

Command Interface configuration mode.

Mode

Usage Guide Use **show mac-address-table notification interface** to display configuration.

Configuration Examples The following example enables the MAC address trap notification on interface gigabitethernet 0/1 when a MAC address is added.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# snmp trap mac-notification added
```

The following example enables the MAC address trap notification on interface gigabitethernet 0/1 when a MAC address is deleted.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# snmp trap mac-notification removed
```

Related Commands

Command	Description
mac-address-table notification	Enables MAC address notification.
show mac-address-table notification	Displays the MAC address notification configuration and the MAC address notification table.

Platform Description N/A

3 Aggregate Port Commands

3.1 aggregateport capacity mode

Use this command to configure the AP capacity mode. Use the **no** form of this command to restore the default setting, Use the **no** form of this command to restore the default setting,

aggregateport capacity mode *capacity-mode*

no aggregateport capacity mode

Parameter	Parameter	Description
Description	<i>capacity-mode</i>	Configures the capacity mode.

Defaults The default *capacity-mode* varies with the device.

Command Mode Global configuration mode

Usage Guide The system provides several capacity modes for devices that support capacity mode configuration. To select a capacity mode, run the **aggregateport capacity mode** *capacity-mode* command in the global configuration mode. To restore the default settings, run **no aggregateport capacity mode** in global configuration mode.

Configuration The following example configures the the capacity mode.

Examples

```
Ruijie# configure terminal
Ruijie(config)# aggregateport capacity mode 8*8
```

Related Commands	Command	Description
	show running	Displays the configuration
	show aggregateport capacity	Displays the current AP capacity mode and use.

Platform N/A

Description

3.2 aggregateport load-balance

Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the **no** form of this command to return the default setting.

aggregateport load-balance { **dst-ip** | **dst-l4port** | **dst-mac** | **src-dst-ip** | **src-dst-l4port** | **src-dst-mac** | **src-ip** | **src-l4port** | **src-mac** }

no aggregateport load-balance

Parameter	Parameter	Description
Description	dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
	dst-l4port	Load balance based on the L4 destination port number. Packets with different L4 destination port numbers are allocated among member links in a balanced way. Packets with the same L4 destination port numbers are allocated to the specific member links.
	dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
	src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
	src-dst-l4port	Load balance based on the L4 source port number and L4 destination port number. Packets with different L4 source+destination port numbers are allocated among member links in a balanced way. Packets with the same L4 source+destination port numbers are allocated to the specific member links.
	src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.
	src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
	src-l4port	Load balance based on the L4 source port number. Packets with different L4 source port numbers are allocated among member links in a balanced way. Packets with the same L4 source port numbers are allocated to the specific member links.
	src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.

Defaults Load balancing can be based on source and destination MAC addresses, source and destination IP addresses (applicable to gateways), or the profile of enhanced load balancing (applicable to switches with CB line cards).

Command Global configuration mode/Interface configuration mode

Mode

Usage Guide You can run `aggregateport load-balance` in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run `no aggregateport load-balance` in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.

Configuration Examples The following example configures a load-balance algorithm globally based on the destination MAC address.

```
Ruijie(config)# aggregateport load-balance dst-mac
```

The following example configures a load-balance algorithm on port 1 based on the destination MAC address.

```
Ruijie(config)# interface aggregateport 1
```

```
Ruijie(config-if-AggregatePort 1)# aggregateport load-balance dst-mac
```

Related Commands	Command	Description
	<code>show aggregateport load-balance</code>	Displays aggregate port configuration.

Platform N/A

Description

3.3 aggregateport member linktrap

Use this command to send LinkTrap to aggregate port members. Use the **no** form of this command to restore the default setting.

aggregateport member linktrap

no aggregateport member linktrap

Parameter	Parameter	Description
Description	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide This function cannot be enabled by running the `snmp trap link-status` command in interface configuration mode. However, it can be enabled by running the `aggregateport member linktrap` command in global configuration mode.

Configuration Examples The following example enables the LinkTrap function on the aggregate port members.

```
Ruijie# configure terminal
```

```
Ruijie(config)# aggregateport member linktrap
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.4 interface aggregateport

Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the **no** form of this command to restore the default setting.

interface aggregateport *ap-number*

no interface aggregateport *ap-number*

Parameter	Parameter	Description
Description	<i>ap-number</i>	Aggregate port number.

Defaults The aggregate port is not created by default.

Command Mode Global configuration mode

Usage Guide If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.

Configuration Examples The following example creates AP 5 and enters its interface configuration mode.

```
Ruijie# configure terminal
Ruijie(config)# interfaces aggregateport 5
Ruijie(config-if-Aggregateport 5)#
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

3.5 lacp port-priority

Use this command to set the priority of the LACP AP member port. Use the **no** form of this command to restore the default setting.

lacp port-priority *port-priority*

no lacp port-priority

Parameter Description	Parameter	Description
		<i>port-priority</i>

Defaults The default is 32768.

Command Mode Interface configuration mode

Usage Guide N/A

Configuration Examples This example sets the LACP port priority of interface Gi0/1 to 4096.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lacp port-priority 4096
```

Related Commands	Command	Description
		N/A

Platform Description N/A

3.6 lacp short-timeout

Use this command to configure the short-timeout mode for the LACP AP member port. Use the no form of this command to restore the default setting.

lacp short-timeout

no lacp short-timeout

Parameter Description	Parameter	Description
		N/A

Defaults The default is long-timeout mode.

Command Mode Interface configuration mode

Usage Guide In long-timeout mode, the port sends an LACP packet every 30 seconds. If the packet is not received in 90 seconds, the connection times out.

In short-timeout mode, the port sends an LACP packet every 1 second. If the packet is not received in 3 seconds, the connection times out.

Configuration The following example configures the short-timeout mode for the LACP AP member port.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lacp short-timeout
```

**Related
Commands**

Command	Description
show lacp summary	Displays the current configuration.
show run	

Platform

N/A

Description

3.7 lacp system-priority

Use this command to set the LACP system priority. Use the **no** form of this command to restore the default setting.

lacp system-priority *system-priority*

no lacp system-priority

**Parameter
Description**

Parameter	Description
<i>system-priority</i>	The LACP system priority, in the range from 0 to 65535.

Defaults

The default is 32768.

**Command
Mode**

Global configuration mode.

Usage Guide

Configuration The following example sets the LACP system priority to 4096.

Examples

```
Ruijie(config)# lacp system-priority 4096
```

**Related
Commands**

Command	Description
show lacp summary	Displays the current configuration.

Platform

N/A

Description

3.8 port-group

Use this command to assign a physical interface to be a member port of a static aggregate port or an LACP aggregate port. Use the **no** form of this command to restore the default setting.

port-group *port-group-number*

port-group *key-number* **mode** { **active** | **passive** }

no port-group

Parameter	Parameter	Description
Description	<i>port-group-number</i>	Member group ID of an aggregate port, the interface number of the aggregate port.
	<i>key-number</i>	Member group ID of an LACP aggregate port, the interface number of the LACP aggregate port.
	active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
	passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.

Defaults By default, the physical port does not belong to any aggregate port.

Command Interface configuration mode.

Mode

Usage Guide All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.

Configuration The following example specifies the Ethernet interface 0/3 as a member of the static AP 3.

Examples

```
Ruijie(config)# interface gigabitethernet 0/3
```

```
Ruijie(config-if-GigabitEthernet 0/3)# port-group 3
```

The following example specifies the Ethernet interface 0/3 as a member of the LACP AP4 and set the aggregation mode to active.

```
Ruijie(config)# interface gigabitethernet 0/3
```

```
Ruijie(config-if-GigabitEthernet 0/3)# port-group 4 mode active
```

Related	Command	Description
Commands	show interface aggregateport	Displays the configuration.

Platform N/A

Description

3.9 show aggregateport

Use this command to display the aggregate port configuration.

show aggregateport *aggregate-port-number* [**load-balance** | **summary**]

Parameter	Parameter	Description
Description	<i>aggregate-port-number</i>	Number of the aggregate port.
	load-balance	Displays the load-balance algorithm on the aggregate port.
	summary	Displays the summary of the aggregate port.

Defaults N/A

Command Mode Any mode

Usage Guide If the aggregate port number is not specified, all the aggregate port information will be displayed.

Configuration Examples The following example displays the aggregate port configuration of switches and wireless ACs.

```
Ruijie# show aggregateport 1 summary
AggregatePort  MaxPorts      SwitchPort Mode    Load balance      Ports
-----
Ag1             8             Enabled  ACCESS  dst-mac           Gi0/2
```

Related Commands	Command	Description
	aggregateport load-balance	Configures a load-balance algorithm of AP.

Platform Description N/A

3.10 show lacp summary

Use this command to display the LACP aggregation information.

show lacp summary [*key-number*]

Parameter	Parameter	Description
Description	key-name	LACP AP port number

Defaults N/A

Command Mode Any mode.

Usage Guide If key-number is not specified, all link aggregation information is displayed.

Configuration The following example displays the LACP aggregation information.

Examples

```
Ruijie(config)# show lacp summary 3
System Id:32768,00d0.f8fb.0002
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs.
A - Device is in active mode.      P - Device is in passive mode.
Aggregate port 3:
Local information:
LACP port      Oper   Port   Port
Port   Flags   State  Priority   Key    Number  State
-----
Gi0/1   SA     bndl   4096      0x3    0x1     0x3d
Gi0/2   SA     bndl   4096      0x3    0x2     0x3d
Gi0/3   SA     bndl   4096      0x3    0x3     0x3d
Partner information:
                LACP port      Oper   Port   Port
Port   Flags   Priority   Dev ID   Key    Number  State
-----
Gi0/1   SA     61440    00d0.f800.0002  0x3    0x1     0x3d
Gi0/2   SA     61440    00d0.f800.0002  0x3    0x2     0x3d
Gi0/3   SA     61440    00d0.f800.0002  0x3    0x3     0x3d
```

Field	Description
Local information	Displays the local LACP information.
Port	Displays the system port ID.
Flags	Displays the port state flag: "S" indicates that the LACP is stable and in the state of periodically sending the LACPPDU; "A" indicates that the port is in the active mode.
State	Show the port aggregation information: "bndl" indicates that the port is aggregated; "Down" represents the disconnection port state; "susp" indicates that the port is not aggregated.
LACP Port Priority	Displays the LACP port priority.
Oper Key	Displays the port operation key.
Port Number	Displays the port number.
Port State	Displays the flag bit for the LACP port state.
Partner information	Partly Displays the LACP information of the peer port.
Dev ID	Partly Displays the system MAC information of the peer device.

Related Commands

Command	Description
port-group key mode	Enables the LACP on the port and specifies the

	aggregation group ID and operation mode.
--	------------------------------------------

Platform N/A

Description

4 VLAN Commands

4.1 add

Use this command to add one or a group Access interface into current VLAN. Use the **no** or **default** form of the command to remove the Access interface.

add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

no add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

default add interface { *interface-type interface-number* | **range** *interface-type interface-range* }

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Layer-2 Ethernet interface or layer-2 AP port.
	range <i>interface-type interface-range</i>	Range of the Layer-2 Ethernet interface or layer-2 AP port.

Defaults All layer-2 Ethernet interfaces are in the VLAN1.

Command mode VLAN configuration mode.

Usage Guide This command is only valid for the access port.

The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the **switchport access vlan** *vlan-id* command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect.

The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.

Configuration Examples The following example adds the interface GigabitEthernet 0/10 to VLAN20.

```
Ruijie# configure terminal
Ruijie(config)# vlan 20
Ruijie(config-vlan)# add interface GigabitEthernet 0/10
Ruijie# show interface GigabitEthernet 0/10 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
GigabitEthernet 0/10 enabled ACCESS 20 1 Disabled ALL
```

The following example adds the interface range GigabitEthernet 0/1-10 to VLAN200.

```
Ruijie# configure terminal
Ruijie(config)# vlan 200
Ruijie(config-vlan)# add interface range GigabitEthernet 0/1-10
Ruijie# show vlan
```

```
Ruijie# 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 the AggregatePort10 to VLAN20.

```
Ruijie# configure terminal
Ruijie(config)# vlan 20
Ruijie(config-vlan)# add interface aggregateport 10
Ruijie# show interface aggregateport 10 switchport
Interface Switchport Mode Access Native Protected VLAN lists
-----
AggregatePort 10 enabled ACCESS 20 1 Disabled ALL
```

Related Commands	Command	Description
		show interface <i>interface-type interface-number</i> switchport

Platform N/A
Description

4.2 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>

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 The following example sets the name of VLAN to 10.

```
Examples
Ruijie(config)# vlan 10
Ruijie(config-vlan)# name vlan10
```

Related Commands	Command	Description
		show vlan

Platform N/A

Description

4.3 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>

Defaults N/A

Command mode All modes

Usage Guide N/A

Configuration The following command displays the status of VLAN 1.

```
Examples
Ruijie(config)# show vlan id 20
VLAN Name                Status   Ports
-----
20 VLAN0020              STATIC  Gi0/1
```

The following command displays the status of all VLANs.

```
Ruijie(config-vlan)# show vlan
VLAN Name                Status   Ports
-----
1 VLAN0001              STATIC  Gi0/1, Gi0/2, Gi0/4, Gi0/5
                               Gi0/6, Gi0/7, Gi0/8, Gi0/9
                               Gi0/10, 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
2 VLAN0002          STATIC   Gi0/1
20 VLAN0020        STATIC   Gi0/1
    
```

Related Commands

Command	Description
name	VLAN name.
switchport access	Adds the interface to a VLAN.

Platform N/A
Description

4.4 switchport access

Use this command to configure an interface as a static access port and assign it to a VLAN. Use the **no** or **default** form of the command to assign the port to the default VLAN.

switchport access vlan *vlan-id*

no switchport access vlan

default switchport access vlan

Parameter Description

Parameter	Description
<i>vlan-id</i>	The VLAN ID at which the port to be added, in the range from 1 to 4094.

Defaults By default, the switch port is an access port and the VLAN is VLAN 1.

Command mode Interface configuration mode.

Usage Guide The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN.
 If the port is a trunk port, the operation does not take effect.

Configuration Examples

```

Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport access vlan 2
    
```

Related Commands

Command	Description
switchport mode	Specifies the interface as Layer 2 mode (switch port mode).
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform N/A
Description

4.5 switchport mode

Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or a servicechain port. Use the **no** or **default** form of this command to restore the default setting.

switchport mode { **access** | **trunk** | **hybrid** | **uplink** }

no switchport mode

default switchport mode

Parameter Description	Parameter	Description
	access	Configures the switch port as an access port.
	trunk	Configures the switch port as a trunk port.
	hybrid	Configures the switch port as a hybrid port.
	uplink	Configures the switch port as an uplink port.

Defaults By default, the switch port is an access port.

Command mode Interface configuration mode.

Usage Guide If a switch port is an access port, the port can be added only to one VLAN. You can run the **switchport access vlan** command to specify the VLAN to which the port belongs.

If a switch port is a trunk port, the port is added to all VLANs by default. You can also run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.

If a switch port is an uplink port, the port is added to all VLANs by default. Different from the trunk port, the uplink port sends packets with a tag carried, that is, the tag of packets from default VLANs will not be deleted. You can run the **switchport trunk allowed** command to add the port to or remove the port from a specified VLAN.

If a switch port is a hybrid port, the port is added to all VLANs by default. Different from a trunk port, a hybrid port can be added to a VLAN in tag or untag mode by running the **switchport hybrid allowed** command.

Configuration The following example configures port 1 as an access port.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode access
```

The following example configures port 1 as a trunk port.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

The following example configures port 1 as an uplink port.

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode uplink
The following example configures port 1 as a hybrid port.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

Related Commands

Command	Description
switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.

Platform N/A
Description

4.6 switchport hybrid allowed

Use this command to add the port to the VLAN or remove the port from the VLAN, Use the **no** or **default** form of this command to restore the default setting.

```
switchport hybrid allowed vlan { [ add ] tagged | [ add ] untagged | only tagged | remove } vlist
no switchport hybrid allowed vlan
default switchport hybrid allowed vlan
```

Parameter Description

Parameter	Description
add	Adds the port to the VLAN.
<i>vlist</i>	Specifies the VLAN.
only tagged <i>vlist</i>	Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list.
[add] tagged <i>vlist</i>	Adds the port to the VLAN and the VLAN packets going out on the port are tagged with VLAN ID.
[add] untagged <i>vlist</i>	Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID.
remove <i>vlist</i>	Removes the port from the VLAN.

Defaults By default, the hybrid port is in all VLANs. All VLAN packets (except native VLAN packets) going out on the port are tagged with VLAN ID. Native VLAN packets are not tagged with VLAN ID.

Command mode Interface configuration mode

Usage Guide N/A

Configuration The following example adds the hybrid port to VLAN 20 and VLAN 30 and the VLAN packets going out on the port are not tagged with VLAN ID.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan
untagged 20
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan add
untagged 30
```

The following example adds the hybrid port to VLAN 40 and VLAN 50 and the VLAN packets going out on the port are tagged with VLAN ID,

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan tagged
40
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan tagged
50
```

The following example removes the hybrid port from VLAN 20.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan remove
20
```

The following example adds the hybrid port to VLAN 20 and deletes all the other VLANs. The VLAN packets going out on the port are tagged with VLAN ID.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan only
tagged 20
```

Related Commands

Command	Description
show interface [<i>interface-type interface-number</i>]	Displays the configuration.

Platform N/A

Description

4.7 switchport hybrid native

Use this command to configure the native VLAN for the hybrid port. Use the **no** or **default** form of this command to restore the default setting.

switchport hybrid native vlan *vlan-id*

no switchport hybrid native vlan
default switchport hybrid native vlan

**Parameter
Description**

Parameter	Description
<i>vlan-id</i>	Configures the native VLAN for the hybrid port, in the range from 1 to 4094.

Defaults

The default is VLAN 1.

**Command
mode**

Interface configuration mode

Usage Guide

Native VLAN packets going out on the hybrid port are not tagged with VLAN ID. Packets not tagged with VLAN ID coming in on the hybrid port are taken as native VLAN packets.

Configuration

The following example configures VLAN 20 as the native VLAN for hybrid port GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode hybrid
Ruijie(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 20
```

**Related
Commands**

Command	Description
N/A	N/A

Platform

N/A

Description

4.8 switchport trunk allowed vlan

Use this command to add the trunk/uplink port to the VLAN or remove a trunk/uplink port from the VLAN. Use the **no** or **default** form of the command to restore the default setting.

switchport trunk allowed vlan { all | add *vlan-list* | remove *vlan-list* | except *vlan-list* | only *vlan-list* }

no switchport trunk allowed vlan

default switchport trunk allowed vlan

**Parameter
Description**

Parameter	Description
all	Adds the trunk/uplink port to all VLANs.
<i>vlan-list</i>	Specifies the VLAN.
add <i>vlan-list</i>	Adds the trunk/uplink port to the specified VLANs.
remove <i>vlan-list</i>	Removes the trunk/uplink port from the specified VLANs.

except <i>vlan-list</i>	Removes the trunk/uplink port from the specified VLANs and adds the port to all the other VLANs.
only <i>vlan-list</i>	Adds the trunk/uplink port to the specified VLANs and removes the port from the VLANs not on the VLAN list.

Defaults The trunk/unlink port is in all VLANs by default.

Command mode Interface configuration mode.

Usage Guide A trunk/uplink port transmits all VLAN (1-4094) data by default. You can block some VLAN data by configuring this command. Use the **show interfaces** command to display configuration.

Configuration Examples The following example removes the trunk port GigabitEthernet 0/10 from VLAN 2.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
2
```

The following example adds the trunk port GigabitEthernet 0/10 to all VLANs except VLAN 10.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except
10
```

The following example adds the trunk port GigabitEthernet 0/10 to VLAN 10 and removes other VLANs.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except
10
```

The following example removes uplink port GigabitEthernet 0/10 from VLAN 10.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove
10
```

The following example adds uplink port GigabitEthernet 0/10 to all VLANs except VLAN10.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except
10
```

The following example adds the uplink port GigabitEthernet 0/10 to VLAN 10 and removes other VLANs.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan only 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.9 switchport trunk native vlan

Use this command to configure the native VLAN for the trunk/uplink port. Use the **no** or **default** form of this command to restore the default setting.

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

default switchport trunk native vlan

Parameter Description	Parameter	Description
		<i>vlan-id</i>

Defaults By default, the native VLAN for the trunk/uplink port is VLAN 1.

Command mode Interface configuration mode

Usage Guide After this function is enabled, packets not tagged with VLAN ID are taken as native VLAN packets. Tags are removed from native VLAN packets going out on the trunk port.

Configuration Examples The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/10.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

The following example configures VLAN 10 as the native VLAN for unlinK port GigabitEthernet 0/10.

```
Ruijie(config)# interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport mode uplink
Ruijie(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A
Description

4.10 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* }

Parameter Description

Parameter	Description
<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094. Default VLAN (VLAN 1) cannot be removed.
range <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.

```
Ruijie(config)# vlan 10
Ruijie(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays member ports of the VLAN.

Platform Description N/A

5 MAC VLAN Commands

5.1 mac-vlan enable

Use this command to enable the MAC VLAN function on the port.

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

mac-vlan enable

no mac-vlan enable

default mac-vlan enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults By default, MAC VLAN is disabled.

Command mode Interface configuration mode

Usage Guide The MAC VLAN entries configured globally will not take effect on the port unless the MAC VLAN function is enabled on this port.
The MAC VLAN function can be enabled on the hybrid port only.

Configuration The following example enables MAC VLAN.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mac-vlan enable
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.2 mac-vlan mac-address

Use this command to configure the static MAC VLAN entries.

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

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id*

no mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id*

default mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id*

Parameter Description	Parameter	Description
	<i>mac-address</i>	Specifies the MAC address.
	mask <i>mac-mask</i>	Specifies the MAC address mask, with the high bits being all 1 in binary. This field is full of F by default.
	vlan <i>vlan-id</i>	Specifies the VLAN corresponding to the MAC address. The range is from 1 to 4,094.

Defaults No static MAC VLAN entry is configured by default.

Command mode Global configuration mode

Usage Guide Use this command to configure a static MAC VLAN entry including the MAC address and VLAN ID. Use the **no** form of this command to remove the static MAC VLAN entry.

Configuration The following example configures a static MAC VLAN entry.

Examples

```
Ruijie(config)# mac-vlan mac-address 0001.0001.0001 vlan 100
Ruijie(config)# mac-vlan mac-address 0002.0002.0000 mask ffff.ffff.0000 vlan 200
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

5.3 show mac-vlan

Use this command to display the MAC VLAN entries.

```
show mac-vlan { all | dynamic | static | vlan vlan-id | mac-address mac-address [ mask mac-mask ] }
```

Parameter Description	Parameter	Description
	all	Displays all MAC VLAN entries.
	dynamic	Displays the dynamic MAC VLAN entries.
	static	Displays the static MAC VLAN entries.
	vlan <i>vlan-id</i>	Displays the MAC VLAN entry of the specified VLAN.
	mac-address <i>mac-address</i>	Displays the MAC VLAN entry of the specified MAC address.
	mask <i>mac-mask</i>	Displays the MAC VLAN entry of the specified MAC address range.

Defaults N/A

Command mode All configuration modes

Usage Guide If the **mac-address** parameter is specified without the **mask** parameter, the MAC-VLAN entry of the single MAC address is displayed.
If parameters both of **mac-address** and **mask** are specified, the MAC-VLAN entries in the specified MAC address range are displayed.

Configuration The following example displays all MAC VLAN entries.

Examples

```
Ruijie# show mac-vlan all
The following MAC VLAN addresses exist:
S: Static D: Dynamic
MAC ADDR          MASK                VLAN ID  PRIO  STATE
-----
0011.1100.0000    ffff.ff00.0000     100      1     S
0022.2222.0000    ffff.ffff.0000     200      2     S
0000.0000.0003    ffff.ffff.ffff     300      3     D
0000.0000.0004    ffff.ffff.ffff     400      4     D
0000.0000.0005    ffff.ffff.ffff     500      5     S&D
0000.0000.0006    ffff.ffff.ffff     600      6     S
0000.0000.0007    ffff.ffff.ffff     700      7     S&D
Total MAC VLAN address count: 7
```

Related Commands

Command	Description
N/A	N/A

Platform N/A

Description

5.4 show mac-vlan interface

Use this command to display the interfaces which are enabled with MAC VLAN.

show mac-vlan interface

Parameter Description

Parameter	Description
N/A	N/A

Defaults N/A

Command All configuration modes

mode

Usage Guide Use this command to verify whether the MAC VLAN function is enabled on the interface.

Configuration The following example displays the interfaces which are enabled with MAC VLAN.

Examples

```
Ruijie# show mac-vlan interface
MAC VLAN is enabled on following interface:
-----
GigabitEthernet 0/3
GigabitEthernet 0/10
```

**Related
Commands**

Command	Description
N/A	N/A

Platform N/A
Description

6 Protocol VLAN Commands

6.1 protocol-vlan profile frame-type

Use this command to configure the profile for the VLAN.

protocol-vlan profile *num* **frame-type EtherII ether-type** *type*

Use this command to delete the specified profile.

no protocol-vlan profile *num*

Use this command to delete all profiles.

no protocol-vlan profile

Parameter Description	Parameter	Description
	profile <i>num</i>	Profile indexes, in the range from 1 to 16
	EtherII ether-type <i>type</i>	Ethernet II message

Defaults It is disabled by default.

Command mode Global configuration mode.

Usage Guide N/A

Configuration Examples The following example configures the profile for the VLAN.

```
Ruijie(config)# protocol-vlan profile 1 frame-type ETHERII ether-type aarp
```

Related Commands	Command	Description
	show protocol-vlan profile	N/A
	show protocol-vlan profile <i>num</i>	N/A
	no protocol-vlan profile	N/A
	no protocol-vlan profile <i>num</i>	N/A

Platform Description N/A

6.2 protocol-vlan profile vlan

Use this command to apply some profile to an interface.

protocol-vlan profile *num* **vlan** *vlan-id*

Use this command to clear the specified profile on the port.

no protocol-vlan profile *vlan-id*

Use this command to clear all profiles on the port.

no protocol-vlan profile

Parameter Description	Parameter	Description
	profile <i>num</i>	Profile indexes,in the range from 1 to 16
	vlan <i>vlan-id</i>	VLAN ID, the maximal VLAN the product supports.

Defaults This function is disabled by default.

Command mode Interface EXEC mode.

Usage Guide N/A

Configuration Examples The following example applies profile 1 to VLAN 101.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/1)# protocol-vlan profile 1 vlan 101
```

Related Commands	Command	Description
	show protocol-vlan profile	N/A
	show protocol-vlan profile <i>num</i>	N/A
	no protocol-vlan profile	N/A
	no protocol-vlan profile <i>num</i>	N/A

Platform N/A

Description

6.3 show protocol-vlan

Use this command to display a protocol VLAN.

show protocol-vlan [profile [*num*]]

Parameter Description	Parameter	Description
	<i>num</i>	Profile index.

Defaults N/A

Command mode Privileged EXEC mode.

Usage Guide N/A

Configuration The following example displays the configuration of protocol VLAN.

Examples

```
Ruijie#show protocol-vlan

profile frame-type      ether-type/DSAP+SSAP  interface  vlan
-----
1          ETHERII      0x5fa        Gi0/1      12
```

**Related
Commands**

Command	Description
N/A	N/A

**Platform
Description**

7 Private VLAN Commands

7.1 private-vlan

Use this command to configure the private VLAN feature. Use the **no** or **default** form of this command to restore the default setting.

private-vlan { **community** | **isolated** | **primary** }

no private-vlan { **community** | **isolated** | **primary** }

default private-vlan { **community** | **isolated** | **primary** }

Parameter Description

Parameter	Description
community	Sets the community VLAN.
isolated	Sets the isolated VLAN.
primary	Sets the primary VLAN.

Defaults No private VLAN feature is configured by default.

Command mode VLAN configuration mode

Usage Guide N/A

Configuration Examples The following example configures the private VLAN feature.

```
Ruijie(config)# vlan 90
Ruijie(config-vlan)# private-vlan primary
Ruijie(config-vlan)# vlan 91
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# vlan 92
Ruijie(config-vlan)# private-vlan community
```

The following example disables the private VLAN feature using the **no private-vlan** command.

```
Ruijie(config)# vlan 90
Ruijie(config-vlan)# no private-vlan primary
Ruijie(config-vlan)# vlan 91
Ruijie(config-vlan)# no private-vlan isolated
Ruijie(config-vlan)# vlan 92
Ruijie(config-vlan)# no private-vlan community
```

The following example disables the private VLAN feature using the **default private-vlan** command.

```
Ruijie(config)# vlan 90
Ruijie(config-vlan)# default private-vlan primary
Ruijie(config-vlan)# vlan 91
Ruijie(config-vlan)# default private-vlan isolated
```

```
Ruijie(config-vlan)# vlan 92
Ruijie(config-vlan)# default private-vlan community
```

Related Commands

Command	Description
N/A	N/A

Platform N/A
Description

7.2 private-vlan association

Use this command to associate the secondary VLAN with the primary VLAN on layer 2. Use the **no** or **default** form of this command to restore the default setting.

private-vlan association { *svlist* | **add** *svlist* | **remove** *svlist* }

no private-vlan association

defaultprivate-vlan association

Parameter Description

Parameter	Description
<i>svlist</i>	The secondary VLAN list
add <i>svlist</i>	Adds the associated secondary VLAN.
remove <i>svlist</i>	Removes the associated secondary VLAN.

Defaults This function is disabled by default.

Command mode VLAN configuration Mode.

Usage Guide This command must be configured in the primary VLAN. Only isolated and community VLANs can be associated.

Configuration The following example associates the secondary VLAN with the primary VLAN on layer 2.

Examples

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association add 24-26
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform N/A
Description

7.3 switchport mode private-vlan

Use this command to declare the private VLAN mode of the interface. Use the **no** or **default** form of this command to restore the default setting.

switchport mode private-vlan { host | promiscuous }

no switchport mode

defaultswitchport mode

Parameter Description	Parameter	Description
	host	Host mode of the private VLAN
	promiscuous	Promiscuous mode of the private VLAN

Defaults The port is an access port by default.

Command mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example declares the private VLAN mode of the interface.

Examples

```
Ruijie(config)# interface gigabitEthernet0/2
Ruijie(config-if-GigabitEthernet 0/2)# switchport mode private-vlan host
```

Related Commands	Command	Description
	show vlan private-vlan	N/A

Platform N/A

Description

7.4 switchport private-vlan host-association

Use this command to associate Layer-2 ports with PVLAN and allocates ports to subdomains. Use the **no** or **default** form of this command to restore the default setting.

switchport private-vlan host-association p_vid s_vid

no switchport private-vlan host-association

defaultswitchport private-vlan host-association

Parameter Description	Parameter	Description
	<i>p_vid</i>	Primary VID, in the range from 2 to 4094
	<i>s_vid</i>	Secondary VID, in the range from 2 to 4094

Defaults This function is disabled by default.

Command mode Interface configuration mode.

Usage Guide N/A

Configuration The following example associates the secondary VLAN with the primary VLAN on the host port.

Examples

```
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan primary
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 23
Ruijie(config-vlan)# private-vlan isolated
Ruijie(config-vlan)# exit
Ruijie(config)# vlan 22
Ruijie(config-vlan)# private-vlan association add 23
Ruijie(config-vlan)# exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode private-vlan host
Ruijie(config-if-GigabitEthernet 0/1)# switchport private-vlan
host-association 22 23
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform N/A

Description

7.5 switchport private-vlan mapping

Use this command to configure the primary VLAN to which a PVLAN promiscuous port belongs and a list of secondary VLANs. Use the **no** or **default** form of this command to restore the default setting.

switchport private-vlan mapping *p_vid* { *svlist* | **add** *svlist* | **remove** *svlist* }

no switchport private-vlan mapping

defaults witchport private-vlan mapping

Parameter Description

Parameter	Description
<i>p_vid</i>	Primary VID, in the range from 2 to 4094
<i>svlist</i>	Secondary VLAN list.
add <i>svlist</i>	Adds the associated secondary VLAN.
remove <i>svlist</i>	Removes the associated secondary VLAN.

Defaults This function is disabled by default.

Command mode Hybrid interface configuration mode of private VLAN

Usage Guide N/A

Configuration The following example configures the secondary VLAN for the hybrid port.

Examples

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport mode private-vlan
promiscuous
Ruijie(config-if-GigabitEthernet 0/1)# switchport private-vlan mapping 22 add
23-25
```

Related Commands

Command	Description
show vlan private-vlan	N/A

Platform N/A
Description

7.6 show vlan private-vlan

Use this command to display the private VLAN configuration.

show vlan private-vlan [community | primary | isolated]

Parameter Description

Parameter	Description
primary	Displays the primary VLAN information.
community	Displays the community VLAN information.
isolated	Displays the isolated VLAN information.

Defaults N/A

Command mode All modes

Usage Guide N/A

Configuration The following example displays the private VLAN configuration.

Examples

```
Ruijie# show vlan private-vlan
VLAN Type      Status  Routed  Ports  Associated VLANs
-----
```


21	isolated	inactive	Disabled	Gi0/8, Gi0/13	No Association
22	community	inactive	Disabled	Gi0/8, Gi0/13	No Association
110	primary	active	Disabled	Gi0/8, Gi0/13	120
120	isolated	active	Disabled	Gi0/8, Gi0/13	110

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

8 Voice VLAN Commands

8.1 show voice vlan

Use this command to display the Voice VLAN configurations and the current state, including the working mode of the port with Voice VLAN enabled.

show voice vlan

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 Voice VLAN configurations and the current state.

Examples

```
Ruijie(config)# show voice vlan
Voice VLAN status: ENABLE //Voice VLAN is enabled
Voice VLAN ID: 2 //Voice VLAN ID
Voice VLAN security mode: Security //Security Mode
Voice VLAN aging time: 5 minutes //Aging Time
Current voice vlan enabled port mode: // Voice VLAN Enabled Port & Mode
PORT MODE
-----
Gi0/1 Auto
```

Related Commands	Command	Description
	voice vlan <i>vlan-id</i>	Sets a voice vlan.
	voice vlan aging <i>minutes</i>	Sets the Voice VLAN aging time.
	voice vlan enable	Enables the Voice VLAN.
	voice vlan mode auto	Sets the Voice VLAN working mode.
	Voice vlan security enable	Enables the Voice VLAN security mode.

Platform Description N/A

8.2 show voice vlan oui

Use this command to display the OUI address, OUI mask and the description information.

show voice vlan oui

Parameter Description	Parameter	Description
	N/A	N/A

Defaults All modes.

Command mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example displays the OUI address.

```

Examples Ruijie(config)# show voice vlan oui
OUI           Mask           Description
-----
0001.e300.0000 ffff.ff00.0000 Siemens phone
0003.6b00.0000 ffff.ff00.0000 Cisco phone
0004.0d00.0000 ffff.ff00.0000 Avaya phone
0060.b900.0000 ffff.ff00.0000 Philips/NEC phone
00d0.1e00.0000 ffff.ff00.0000 Pingtel phone
00e0.7500.0000 ffff.ff00.0000 Polycom phone
00e0.bb00.0000 ffff.ff00.0000 3com phone
    
```

The following lists the field description .

Field	Description
OUI	The OUI address, the source MAC address for the voice packet.
Mask	The OUI mask. The valid length for the OUI address.
Description	The description information for the OUI address.

Related Commands	Command	Description
	voice vlan mac-address <i>mac-addr</i> mask <i>oui-mask</i> [description <i>text</i>]	Sets the OUI address for the voice packet recognized by the Voice VLAN.

Platform Description N/A

8.3 voice vlan

Use this command to enable Voice VLAN in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan *vlan-id*






no voice vlan

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The Voice VLAN ID.

Defaults This function is disabled by default.

Command mode Global configuration mode

Usage Guide Use this command to enable the Voice VLAN and specify the Voice VLAN ID.

-  1. The corresponding VLAN shall be created before configuring the Voice VLAN;
-  2. The default VLAN is VLAN1 and cannot be set as the Voice VLAN;
-  3. A VLAN is not allowed to be set as the Voice VLAN and the Super VLAN at the same time;
-  4. With 802.1x VLAN auto-switching function enabled, the assigned VID shall not be set as the Voice VLAN ID;
-  5. RSPAN Remote VLAN and Voice VLAN cannot be the same VLAN, or it influences the remote port mirror and the Voice VLAN function.

Configuration The following example sets the VLAN2 as the Voice VLAN.

```
Ruijie(config)# vlan 2
Ruijie(config-vlan)# exit
Ruijie(config)# voice vlan 2
```

Related Commands	Command	Description
	show voice vlan	Displays Voice VLAN configurations and the current state.

Platform N/A
Description

8.4 voice vlan aging

Use this command to set the Voice VLAN aging time in the global configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan aging *minutes*
no voice vlan aging

**Parameter
Description**

Parameter	Description
<i>minutes</i>	The Voice VLAN aging time. Range: 5 to 10,000. Unit: minute.

Defaults The default is 1440 minutes.

**Command
mode** Global configuration mode

Usage Guide If the device has not received any voice packets from the port within the aging time, this Voice VLAN will be removed from this port.

 The aging time is valid for the auto-mode only.

Configuration The following example sets the Voice VLAN aging time to 10 minutes.

Examples Ruijie(config)# voice vlan aging 10

**Related
Commands**

Command	Description
show voice vlan	Displays Voice VLAN configurations and the current state.

**Platform
Description** N/A

8.5 voice vlan enable

Use this command to enable the Voice VLAN DSCP value in the interface configuration mode. Use the **no** form of this command to restore the default setting.

voice vlan enable
no voice vlan enable

**Parameter
Description**

Parameter	Description
N/A	N/A

Defaults This function is disabled by default.

**Command
mode** Interface configuration mode

Usage Guide Use this command to enable the Voice VLAN on the physical port only. The Voice VLAN can be

enabled on the Access Port, Trunk Port, Hybrid Port, Private VLAN host port, and Private VLAN promiscuous port and Uplink port on the Ruijie products.

i With the global Voice VLAN disabled, although the Voice VLAN can be enabled on the port, it is invalid.

Configuration The following example enables the Voice VLAN function on the interface GigabitEthernet 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# voice vlan enable
```

**Related
Commands**

Command	Description
show voice vlan	Displays Voice VLAN configurations and the current state.

Platform N/A

Description

8.6 voice vlan mac-address

Use this command to set the recognizable Voice VLAN OUI address. Use the **no** form of this command to restore the default setting.

voice vlan mac-address *mac-addr* **mask** *oui-mask* [**description** *text*]

no voice vlan mac-address *mac-addr*

**Parameter
Description**

Parameter	Description
<i>mac-addr</i>	In the format of <i>H.H.H</i> . The source MAC address for the voice packets.
mask <i>oui-mask</i>	In the format of <i>H.H.H</i> . The valid length for the OUI address.
description <i>text</i>	The description for the OUI address.

Defaults By default, no OUI has been configured.

Command mode Global configuration mode

Usage Guide Use this command to identify the voice packets from different manufacturers. The first three bytes of the MAC address for the voice device are used to identify the manufacture. Voice VLAN determines whether the packets are voice packets or not through the OUI address obtained from the source MAC address and the OUI mask for the received packets.

i The Voice VLAN OUI address cannot be the multicast address and the configured mask shall be continuous.

Configuration Examples The following example sets the OUI address 0012.3400.0000 as the valid address for the Voice VLAN.

```
Ruijie(config)# voice vlan mac-address 0012.3400.0000 mask ffff.ff00.0000
description Company-A
```

Related Commands

Command	Description
show voice vlan oui	Displays the OUI address, OUI address mask and the descriptions.

Platform Description N/A

8.7 voice vlan mode auto

Use this command to set the Voice VLAN auto mode. Use the **no** form of this command to disable this function.

voice vlan mode auto

no voice vlan mode auto




Parameter Description


Parameter	Description
N/A	N/A

Defaults This function is in auto mode by default.

Command mode Interface configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

-  1. With the Voice VLAN enabled on the port and in the manual mode, this port must be added to the Voice VLAN manually to ensure the function validity.
-  2. When the port works in the auto-mode, note that the native VLAN of the port cannot be set as the Voice VLAN for the normal function performance.
-  3. The Trunk Port/Hybrid Port on the Ruijie product can transmit the packets in all VLANs by default. First remove the Voice VLAN from the allowed VLAN list for the port, then enable the Voice VLAN to ensure that the port disconnecting with the voice device cannot be added to the Voice VLAN, or the port not used for a long time can be still in the Voice VLAN.

-  1. With the Voice VLAN enabled on the port, the auto and manual modes switchover is disallowed. Disable the Voice VLAN first if it is necessary to switch the modes.
- 2. In the auto mode, it fails to add/remove the port to/from the Voice Vlan by using the command.

Configuration Examples The following example sets the Voice VLAN on the interface GigabitEthernet 0/1 to work in the auto mode.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-vlan)# voice vlan mode auto
```

Related Commands

Command	Description
show voice vlan	Displays Voice VLAN configurations and the current state.

Platform N/A

Description

8.8 voice vlan security enable

Use this command to enable the Voice VLAN security mode in the global configuration mode. Use the **no** form of this command to disable this function.

voice vlan security enable

no voice vlan security enable


Parameter Description

Parameter	Description
N/A	N/A

Defaults This function is enabled by default.

Command mode Global configuration mode

Usage Guide The Voice VLAN working mode can be classified into the auto-mode and the manual-mode, and configured on the port. The working modes for the Voice VLAN on each port are independent, and different ports can work in different working modes. In different working modes, the methods of enabling the Voice VLAN function on the port are different. The working mode can be set according to the IP phone type connected downward the port or the port type.

-  You are not recommended to transmit the voice and service data in the Voice VLAN at the same time. But if it is necessary for you, you shall ensure that the Voice VLAN security mode has been disabled.

i In the security mode, only the source MAC addresses for the untagged packets and the packets carried with Voice VLAN tag are checked. For other packets carried with non-voice vlan tag that free from the Voice VLAN security/normal mode, the devices forward or discard those packets according to the VLAN rule.

Configuration The following example enables the Voice VLAN security mode.

Examples `Ruijie(config)# voice vlan security enable`

Related Commands	Command	Description
		<code>show voice vlan</code>

Platform N/A

Description

9 VLAN Mapping Commands

9.1 show interfaces vlan-mapping

Use this command to display the VLAN mapping configuration.

show interfaces [*interface-type interface-number*] **vlan-mapping**

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	The interface (access, trunk, hybrid or uplink port) configured with the VLAN mapping function

Defaults N/A

Command Mode Any mode

Usage Guide N/A

Configuration Examples The following example displays the VLAN mapping configuration.

```
ruijie# show interfaces vlan-mapping
Ports          Type      Status Destination-VID Source-VID-list
-----
Gi0/1         out      active      3              5
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

9.2 vlan-mapping-out vlan src-vlan remark dest-vlan

Use this command to configure the policy list of the one-to-one VLAN mapping in the outgoing direction on the access, trunk, hybrid, uplink port. Use the **no** or **default** form of this command to restore the default setting.

vlan-mapping-out vlan *src-vlan* **remark** *dest-vlan*

no vlan-mapping-out vlan *src-vlan* **remark** *dest-vlan*

default vlan-mapping-out vlan *src-vlan* **remark** *dest-vlan*

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

Description		
	<i>src-vlan</i>	Source VLAN
	<i>dest-vlan</i>	Destination VLAN
	no	Removes the settings.

Defaults The policy list is null by default.

Command Mode Interface configuration mode.

Usage Guide N/A

Configuration Examples The following example changes the destination VLAN of the packet whose source VLAN is 3 to 4 in the outgoing direction of the interface, and then forwards it.

```
Ruijie# configure terminal
Ruijie(config)# vlan range 3-4
Ruijie(config-vlan-range)# exit
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# switchport mode trunk
Ruijie(config-if)# vlan-mapping-out vlan 3 remark 4
```

Related Commands	Command	Description
	show interface [interface-type interface-number] vlan-mapping	Displays the VLAN mapping configuration.

Platform Description N/A

10 STP/RSTP/MSTP Commands

10.1 bpdu src-mac-check

Use this command to enable the BPDU source MAC address check function on the interface. Use the **no** form or **default** form of this command to restore the default setting.

bpdu src-mac-check *H.H.H*

no bpdu src-mac-check

default bpdu src-mac-check

Parameter Description

Parameter	Description
<i>H.H.H</i>	Indicates that only the BPDU messages from this MAC address are received.

Defaults

This function is disabled by default.

Command Mode

Interface configuration mode.

Usage Guide

BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.

Configuration Examples

The following example indicates only the BPDU with 00d0.f800.1e2f as the source MAC address will be received by interface GigabitEthernet 0/1 .

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# bpdu src-mac-check 00d0.f800.1e2f
```

Related Commands

Command	Description
N/A	N/A

Platform Description

N/A

10.2 bridge-frame forwarding protocol bpdu

Use this command to enable BPDU transparent transmission. Use the **no** form or **default** form of this command to restore the default setting.

bridge-frame forwarding protocol bpdu
no bridge-frame forwarding protocol bpdu
default bridge-frame forwarding protocol bpdu

Parameter Description	Parameter	Description
	N/A	N/A

Defaults This function is disabled by default.

Command Mode Global configuration mode

Usage Guide In the IEEE 802.1Q standard, 01-80-C2-00-00-00, the destination MAC address of BPDU frames, is reserved. Devices following the IEEE 802.1Q standard don't forward BPDU frames. In real network deployment, devices may be required to support BPDU transparent transmission. For example, when a device is not enabled with STP, BPDU transparent transmission can help implement STP calculation.
 BPDU transparent transmission works only when STP is disabled.

Configuration Examples The following example enables BPDU transparent transmission.

```
Ruijie(config)# bridge-frame forwarding protocol bpdu
```

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.3 clear spanning-tree counters

Use this command to clear the statistics of the sent and received STP packets.

clear spanning-tree counters [**interface** *interface-type interface-number*]

Parameter Description	Parameter	Description

<i>interface-type interface-number</i>	Interface number
----------------------------------------	------------------

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide It is used to clear the statistics of the sent and received STP packets.

Configuration The following example clears the statistics of the sent and received STP packets.

Examples

```
Ruijie# clear spanning-tree counters
```

The following example clears the statistics of the sent and received packets on interface Gi 0/1.

```
Ruijie# clear spanning-tree counters interface gigabitethernet 0/1
```

Related Commands	Command	Description
	show spanning-tree counters	Displays the statistics of STP transceived packets.

Platform Description N/A

10.4 clear spanning-tree detected-protocols

Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.

clear spanning-tree detected-protocols [interface *interface-type interface-number*]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface number

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide Use this command to force the interface to send the RSTP BPDU message.

Configuration Forces to check the version of all interfaces.

Examples

```
Ruijie# clear spanning-tree detected-protocols
```

Related Commands	Command	Description
------------------	---------	-------------

show spanning-tree interface	Displays the STP configuration of the interface.
-------------------------------------	--------------------------------------------------

Platform N/A

Description

10.5 clear spanning-tree mst topochange record

Use this command to clear STP topology change record.

clear spanning-tree mst *instance-id* topochange record

Parameter	Parameter	Description
Description	<i>instance-id</i>	Instance ID, in the range from 0 to 63. For STP and RSTP protocols, only instance 0 is valid.

Defaults N/A

Command Mode Privileged EXEC mode

Usage Guide N/A

Configuration The following example clears STP topology change record.

Examples

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
Time                Interface          Old status   New status   Type
-----
2013.5.1 4:18:46   GI0/1         Learning    Forwarding   Normal
Ruijie# clear spanning-tree mst 0 topochange record
Ruijie# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

10.6 show spanning-tree

Use this command to display the global spanning-tree configuration.

show spanning-tree [summary | forward-time | hello-time | max-age | inconsistentports |

tx-hold-count | pathcost method | max_hops | counters]

**Parameter
Description**

Parameter	Description
summary	Displays the information of MSTP instances and forwarding status of the interfaces.
inconsistentports	Displays the block port due to root guard or loop guard.
forward-time	Displays BridgeForwardDelay.
hello-time	Displays BridgeHelloTime.
max-age	Displays BridgeMaxAge.
max-hops	Displays the maximum hops of an instance.
tx-hold-count	Displays TxHoldCount.
pathcost method	Displays the method used for calculating path cost.
counters	Displays the statistics of STP transceived packets.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide N/A

Configuration Examples The following example displays the global spanning-tree configuration.

```
Ruijie# show spanning-tree hello-time
```

The following example displays the sent and received STP packets.

```
Ruijie# show spanning-tree counters
```

```
----- STP BPDU count -----
Port                Receive      Send
GigabitEthernet 0/3          0          122594
```

```
----- STP TC or TCN count -----
MSTID  Port                Receive      Send
0      GigabitEthernet 0/3          0            0
```

**Related
Commands**

Command	Description
spanning-tree pathcost method	Sets the pathcost method.
spanning-tree forward-time	Sets BridgeForwardDelay.
spanning-tree hello-time	Sets BridgeHelloTime.
spanning-tree max-age	Sets BridgeMaxAge.
spanning-tree max-hops	Sets the maximum hops of an instance.
spanning-tree tx-hold-count	Displays TxHoldCount.

Platform N/A
Description

10.7 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.

show spanning-tree interface *interface-type interface-number* [**bpdufilter** | **portfast** | **bpduguard** | **link-type**]

Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface number
	bpdufilter	Displays the status of BPDU filter.
	portfast	Displays the status of portfast.
	bpduguard	Displays the status of BPDU guard.
	link-type	Displays the link type of an interface.

Defaults N/A

Command Mode Privileged EXEC mode, global configuration mode and interface configuration mode.

Usage Guide For interfaces in up status, just use the **show spanning-tree interface** *interface* command to display status of all features.
 For interfaces in down status, the feature parameter should be specified to display the status of the specific feature.

Configuration The following example displays the STP configuration on interface Gi 0/1 and .interface Gi 0/2.

Examples

```
Ruijie(config)# show interface description
Interface           Status  Administrative Description
-----
GigabitEthernet 0/1    up      up
GigabitEthernet 0/2    down    up

Ruijie# show spanning-tree int gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast  : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge  : Disabled
PortAdminLinkType : auto
PortOperLinkType  : point-to-point
PortBPDUGuard     : Disabled
```

```

PortBPDUFilter : Disabled
PortGuardmode : None

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort

Ruijie# show spanning-tree interface gi 0/2
no spanning tree info available for GigabitEthernet 0/2.
Ruijie# show spanning-tree interface gi 0/2 bpdudfilter
PortBPDUFilter : Disabled
Ruijie# show spanning-tree interface gi 0/2 portfast
PortAdminPortFast :Disabled
Ruijie # show spanning-tree interface gi 0/2 bpduguard
PortBPDUGuard : Disabled
Ruijie# show spanning-tree interface gi 0/2 link-type
PortAdminLinkType : auto
    
```

Related Commands

Command	Description
spanning-tree bpdudfilter	Enables the BPDU filter feature someone the interface.
spanning-tree portfast	Enables the portfast on the interface.
spanning-tree bpduguard	Enables the BPDU guard on the interface.
spanning-tree link-type	Sets the link type of the interface to point-to-point.

Platform N/A
Description

10.8 show spanning-tree mst

Use this command to display the information of MST and instances.

show spanning-tree mst { configuration | instance-id [interface interface-type interface-number] }

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

Description	
configuration	The MST configuration of the equipment.
<i>instance-id</i>	Instance ID, in the range from 0 to 63.
interface <i>interface-type interface-number</i>	Interface number

Defaults

Command Mode Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide N/A

Configuration The following example displays the information of MST and instances.

Examples

```
Ruijie# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : test
Revision  : 0
Instance  Vlans Mapped
-----
0         : 2-4094
1         : 1
```

Field Description

Field	Description
Multi spanning tree protocol	Enables MSTP protocol.
Name	Name of the MST region
Revision	Revision of the MST region
Instance Vlans Mapped	Mapping relation between the instance and VLAN

Related Commands	Command	Description
	spanning-tree mst configuration	Configures the MST region.
	spanning-tree mst cost	Displays the path cost of the instance.
	spanning-tree mst max-hops	Displays the maximum hops of the instance.
	spanning-tree mst priority	Displays the equipment priority of the instance.
	spanning-tree mst port-priority	Displays the port priority of the instance.

Platform N/A

Description

10.9 show spanning-tree mst topochange record

Use this command to display the STP topology change record.

show spanning-tree mst *instance-id* topochange record

Parameter Description	Parameter	Description
	<i>instance-id</i>	Instance ID, in the range from 0 to 63.

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 STP topology change record of instance 0.

```
Ruijie# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
Time                Interface                Old status    New status    Type
-----
2013.5.1 4:18:46   GI0/6                Learning     Forwarding    Normal
```

Field	Description
Time	The time when the topology changes.
Interface	The interface whose topology changes.
Old status	Old STP status on the interface.
New status	New STP status on the interface.
Type	Topology change may be caused by the following causes: Normal: UP/DOWN state change on the interface, LoopGuard Block: Loop-inconsistence causes the interface to be blocked. RootGuard Block: Root-inconsistence causes the interface to be blocked. Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked. LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence. Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.

Related Commands	Command	Description
	N/A	N/A

Platform Description N/A

10.10 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

spanning-tree [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*]

no spanning-tree [**forward-time** | **hello-time** | **max-age**]

Parameter Description	Parameter	Description
	forward-time <i>seconds</i>	Interval at which the port status changes, in the range from 4 to 30 in the unit of seconds. The default is 15.
	hello-time <i>seconds</i>	Interval at which the switch sends the BPDU message, in the range from 1 to 10 in the unit of seconds. The default is 2.
	max-age <i>seconds</i>	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.

Defaults This function is disabled by default.

Command Mode Global configuration mode.

Usage Guide The values of **forward-time**, **hello time** and **max-age** are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values.
 $2 * (\text{Hello Time} + 1.0\text{snd}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0\text{snd})$
 If the values do not according with the condition, the settings do not work.

Configuration Examples The following example enables the spanning-tree function.

```
Ruijie(config)# spanning-tree
```

The following example configures the BridgeForwardDelay.

```
Ruijie(config)# spanning-tree forward-time 10
```

Related Commands	Command	Description
	show spanning-tree	Displays the global STP configuration.
	spanning-tree mst cost	Sets the PathCost of an STP interface.
	spanning-tree tx-hold-count	Sets the global TxHoldCount of STP.

Platform Description N/A

10.11 spanning-tree autoedge

Use this command to enable Autoedge on the interface. Use the **disabled** form of this command to disable this function.

spanning-tree autoedge [disabled]

Parameter Description	Parameter	Description
	disabled	Disabled Autoedge on the interface.

Defaults This function is enabled by default.

Command Mode Interface configuration mode.

Usage Guide If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.
You can run the spanning-tree autoedge disabled command to disable Auto Edge.

Configuration The following example disables Autoedge on the interface.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree autoedge disabled
```

Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration information of the interface.

Platform Description N/A

10.12 spanning-tree bpdudfilter

Use this command to enable BPDU filter on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU filter function on the interface.

spanning-tree bpdudfilter { enabled | disabled }

Parameter Description	Parameter	Description
	enabled	Enables BPDU filter on the interface.
	disabled	Disables BPDU filter on the interface.

- Defaults** This function is disabled by default,
- Command** Interface configuration mode.
- Mode**
- Usage Guide** If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.

Configuration The following example enables BPDU filter on interface Gi 0/1.

Examples

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree bpdudfilter enable
```

**Related
Commands**

Command	Description
show spanning-tree interface	Displays the STP configuration of the interface.

Platform N/A

Description

10.13 spanning-tree bpduguard

Use this command to enable the BPDU guard function on the interface. You can use the **enabled** or **disabled** option of the command to enable or disable the BPDU guard function on the interface.

spanning-tree bpduguard { enabled | disabled }

**Parameter
Description**

Parameter	Description
enabled	Enables BPDU guard on the interface.
disabled	Disables BPDU guard on the interface.

- Defaults** This function is disabled by default.
- Command** Interface configuration mode.
- Mode**
- Usage Guide**
1. If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
 2. Run command **errdisable recovery [interval seconds]** to recover the interface in Error-disabled state.
- Configuration** The following example enables the BPDU guard function on the interface.
- Examples**
- ```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree bpduguard enable
```

**Related**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                 |                                     |                                                  |
|-----------------|-------------------------------------|--------------------------------------------------|
| <b>Commands</b> |                                     |                                                  |
|                 | <b>show spanning-tree interface</b> | Displays the STP configuration of the interface. |

**Platform** N/A

**Description**

## 10.14 spanning-tree compatible enable

Use this command to send the message selectively carried with MSTI according to the interface attribute of current port to realize interconnection with other vendors. Use the **no** form of this command to restore the default setting.

**spanning-tree compatible enable**

**no spanning-tree compatible enable**

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

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide**

1. If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between Ruijie devices and other SPs' devices. For example:  
spanning-tree mst configuration  
instance 1 vlan 1  
instance 2 vlan 2  
If the interface 1 only belongs to VLAN 1 and STP compatibility mode is enabled, the BPDU packet sent by the interface 1 only carries instance 0 and instance 1.
2. If the compatibility mode is enabled on a port, STP will calculate whether the interface takes part in the specific instance calculation according to interface's VLAN and the mapping between VLAN and instance.
3. Instance 0 (CIST) takes part in calculation by default.

**Configuration** The following example enables the compatibility mode on interface Gi 0/1.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree compatible enable
```

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



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

## 10.15 spanning-tree guard loop

Use this command to enable **loop guard** on the interface to prevent the root port or backup port from generating loop since they cannot receive bpd. Use the **no** form of this command to disable **loop guard**.

**spanning-tree guard loop**  
**no spanning-tree guard loop**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

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

**Command Mode** Interface configuration mode

**Usage Guide**

1. Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.
2. The loop guard function and root guard function cannot be enabled at the same time.

**Configuration Examples** The following example enables **loop guard** on interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree guard loop
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 10.16 spanning-tree guard none

Use this command to disable **guard** on the interface. Use the **no** form of this command to enable this function

**spanning-tree guard none**  
**no spanning-tree guard none**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |     |     |
|--------------------|-----|-----|
| <b>Description</b> |     |     |
|                    | 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 disables **guard** on interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree guard none
```

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

**Platform Description** N/A

## 10.17 spanning-tree guard root

Use this command to enable **root guard** on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the **no** form of this command to restore the default setting.

**spanning-tree guard root**

**no spanning-tree guard root**

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

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

**Command Mode** Interface configuration mode

- Usage Guide**
- If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks.
  - The loop guard function and root guard function cannot be enabled at the same time.

**Configuration Examples** The following example enables **root guard** on the interface.

```
Ruijie(config)# interface gigabitethernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree guard root
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 10.18 spanning-tree ignore tc

Use this command to enable the tc filtering on the interface. Use the **no** form of this command to restore the default setting. With tc filtering enabled, the TC packets received on the interface will not be processed.

**spanning-tree ignore tc**

**no spanning-tree ignore tc**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

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

**Command  
Mode** Interface configuration mode.

**Usage Guide** If TC filter is enabled on a port, the port does not process received TC packets.

**Configuration** The following example enables the tc filtering on the interface.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree ignore tc
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 10.19 spanning-tree link-type

Use this command to configure the link type of the interface. Use the **no** form of this command to restore the default setting.

**spanning-tree link-type { point-to-point | shared }**  
**no spanning-tree link-type**

**Parameter  
Description**

| Parameter             | Description                                             |
|-----------------------|---------------------------------------------------------|
| <b>point-to-point</b> | Sets the link type of the interface to point-to-point.  |
| <b>shared</b>         | Forcibly sets the link type of the interface to shared. |

**Defaults**

For a full-duplex interface, its link type is set to point-to-point; for a half-duplex interface, its link type is set to shared.

**Command**

Interface configuration mode.

**Mode**

**Usage Guide**

If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

**Configuration**

The following example configures the link type of the interface.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree link-type
point-to-point
```

**Related  
Commands**

| Command                             | Description                                      |
|-------------------------------------|--------------------------------------------------|
| <b>show spanning-tree interface</b> | Displays the STP configuration of the interface. |

**Platform**

N/A

**Description**

## 10.20 spanning-tree loopguard default

Use this command to enable **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpd. Use the **no** form of this command to restore the default setting.

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

This function is disabled by default.

**Command**

Global configuration mode.

**Mode**

**Usage Guide** Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.

**Configuration Examples** The following example enables **loop guard** globally to prevent the root port or backup port from generating loop since they cannot receive bpdu.

```
Ruijie(config)# spanning-tree loopguard default
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 10.21 spanning-tree max-hops

Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before being dropped. This parameter takes effect for all instances. Use the **no** form of this command to restore the default setting.

**spanning-tree max-hops** *hop-count*

**no spanning-tree max-hops**

**Parameter Description**

| Parameter        | Description                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------|
| <i>hop-count</i> | Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops. |

**Defaults** The default is 20 hops.

**Command** Global configuration mode.

**Mode**

**Usage Guide** In the region, the BPDU message sent by the root bridge includes a Hop Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the max-hops command affects all instances.

**Configuration Examples** This example sets the max-hops of the spanning tree to 10 for all instances.

```
Ruijie(config)# spanning-tree max-hops 10
```

**Related**

| Command | Description |
|---------|-------------|
|---------|-------------|

| Commands                  |                                |
|---------------------------|--------------------------------|
| <b>show spanning-tree</b> | Displays the MSTP information. |

**Platform** N/A

**Description**

## 10.22 spanning-tree mode

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

**spanning-tree mode { stp | rstp | mstp }**

**no spanning-tree mode**

| Parameter Description | Parameter   | Description                                  |
|-----------------------|-------------|----------------------------------------------|
|                       | <b>stp</b>  | Spanning tree protocol(IEEE 802.1d)          |
|                       | <b>rstp</b> | Rapid spanning tree protocol(IEEE 802.1w)    |
|                       | <b>mstp</b> | Multiple spanning tree protocol(IEEE 802.1s) |

**Defaults** The default is **mstp**.

**Command**

**Mode** Global configuration mode.

**Usage Guide** However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the STP mode to a lower version.

**Configuration** The following example sets the STP version.

**Examples**

```
Ruijie(config)# spanning-tree mode stp
```

| Related Commands | Command                   | Description                               |
|------------------|---------------------------|-------------------------------------------|
|                  | <b>show spanning-tree</b> | Displays the spanning-tree configuration. |

**Platform** N/A

**Description**

## 10.23 spanning-tree mst configuration

Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the **no** form of the command to restore the default setting.

**spanning-tree mst configuration**  
**no spanning-tree mst configuration**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

All VLANs are in instance 0 by default.  
 Name is a null string.  
 Revision is 0.

**Command Mode**

Global configuration mode

**Usage Guide**

This command is MSTP-specific.

To return to the privileged EXEC mode, enter end or Ctrl+C.

To return to the global configuration mode, enter exit.

After entering the MST configuration mode, you can configure parameters by these commands:

**instance** *instance-id* **vlan** *vlan-range*: Add VLAN to MST instance. Instance-ID is in the range from 0 to 63 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8, 9 to instance 10. By default, all VLANs are in instance 0. Use the **no** form of this command to remove VLAN from instance 1-63.

If you create 63 instances by stacking on a Ruijie device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.

**name** *name*: MST name, up to 32 characters are allowed. Run the **no name** command to restore the default settings.

**revision** *version*: MST version number, ranging from 0 to 65535. Run the **no revision** command to restore the default settings.

**show spanning-tree mst configuration**: Displays the current MST region information.

**Configuration**

This example enters the MST configuration mode and maps VLAN 3, 5-10 to MST instance 1.

**Examples**

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# name region1
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
MST configuration
Name [region1]
Revision 1
Instance Vlans Mapped
----- -
```

```
0 1-2, 4, 11-4094
1 3, 5-10

```

```
Ruijie(config-mst)# exit
```

The following example deletes VLAN 3 from instance 1.

```
Ruijie(config-mst)# no instance 1 vlan 3
```

The following example deletes instance 1.

```
Ruijie(config-mst)# no instance 1
```

#### Related Commands

| Command                                                          | Description                            |
|------------------------------------------------------------------|----------------------------------------|
| <b>show spanning-tree mst</b>                                    | Displays the MST region configuration. |
| <b>instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-range</i> | Adds VLANs to the MST instance.        |
| <b>name</b>                                                      | Configures the name of MST.            |
| <b>revision</b>                                                  | Configures the version of MST.         |

**Platform** N/A

**Description**

## 10.24 instance

Use this command to set instance and VLAN mapping relations. Use the **no** form of the command to restore the default setting.

**instance** *instance-id* **vlan** *vlan-range*

**no instance** *instance-id* { **vlan** *vlan-range* }

#### Parameter Description

| Parameter          | Description                              |
|--------------------|------------------------------------------|
| <i>instance-id</i> | Instance ID, in the range from 0 to 63   |
| <i>vlan-range</i>  | VLAN range, in the range from 1 to 4094. |

#### Defaults

The default is instance 0.

#### Command Mode

MST configuration mode

#### Usage Guide

This command is MSTP-specific.

**instance** *instance-id* **vlan** *vlan-range*: Add VLAN to MST instance. Instance-ID is in the range from 0 to 63 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8, 9 to instance 10. By default, all VLANs are in instance 0. Use the no form of this command to remove VLAN from instance 1-63.



If you create 63 instances by stacking on a Ruijie device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.

**Configuration** This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1.

**Examples**

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# instance 1 vlan 3, 5-10
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name :
Revision : 0
Instance Vlans Mapped
----- -----
0 1-2,4,11-4094
1 3,5-10

Ruijie(config-mst)# exit
Ruijie(config)#
```

The following example removes VLAN3 from instance 1.

```
Ruijie(config-mst)# no instance 1 vlan 3
```

The following example removes instance 1.

```
Ruijie(config-mst)# no instance 1
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 10.25 revision

Use this command to set revision number of MSTP region. Use the **no** form of the command to restore the default setting.

**revision** *version*

**no revision**

**Parameter Description**

| Parameter      | Description                                        |
|----------------|----------------------------------------------------|
| <i>version</i> | MST revision number, in the range from 0 to 65535. |

**Defaults** The default is 0.

**Command Mode** MST configuration mode

**Usage Guide** This command is MSTP-specific.

**revision** *version*: Sets the MST version, in the range from 0 to 65535.

**show spanning-tree mst configuration**: Displays MST region information.

**Configuration** This example sets revision number to 1.

```
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# revision 1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name :
Revision : 1
Instance Vlans Mapped

0 : ALL
Ruijie(config-mst)# exit
Ruijie(config)#
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 10.26 name

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

**name** *name*  
**no name**

**Parameter  
Description**

| Parameter   | Description                    |
|-------------|--------------------------------|
| <i>name</i> | MST name, up to 32 characters. |

**Defaults** The default is NULL.

**Command** MST configuration mode

**Mode**

**Usage Guide** This command is MSTP-specific.

**name** *name*: Sets the MST name, up to 32 characters.

**show spanning-tree mst configuration**: Displays MST region information.

**Configuration** This example sets MST name to region1.

```

Examples
Ruijie(config)# spanning-tree mst configuration
Ruijie(config-mst)# name region1
Ruijie(config-mst)# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name : region1
Revision : 0
Instance Vlans Mapped

0 : ALL
Ruijie(config-mst)# exit
Ruijie(config)#

```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 10.27 spanning-tree cost

Use this command to set the path cost of an instance in the interface configuration mode. Use the **no** form of the command to restore the default setting.

**spanning-tree [ mst *instance-id* ] cost *cost***

**no spanning-tree [ mst *instance-id* ] cost**

**Parameter  
Description**

| Parameter          | Description                                   |
|--------------------|-----------------------------------------------|
| <i>instance-id</i> | Instance ID in the range from 0 to 63.        |
| <i>cost</i>        | Path cost in the range from 1 to 200,000,000. |

**Defaults** The default instance-id is 0.  
The default value is calculated by the link rate of the interface automatically.  
1000 Mbps—20000  
100 Mbps—200000  
10 Mbps—2000000

**Command** Interface configuration mode.  
**Mode**

**Usage Guide** This command is MSTP-specific.  
A higher cost value means a higher path cost.

**Configuration** This example sets the path cost to 400 on the interface associated with instances 3.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree mst 3 cost 400
```

| Related<br>Commands | Command                                | Description                                    |
|---------------------|----------------------------------------|------------------------------------------------|
|                     | <b>show spanning-tree mst</b>          | Displays the MSTP information of an interface. |
|                     | <b>spanning-tree mst port-priority</b> | Configures the priority of an interface.       |
|                     | <b>spanning-tree mst priority</b>      | Configures the priority of an instance.        |

**Platform** N/A

**Description**

## 10.28 spanning-tree port-priority

Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the **no** form of this command to restore the default setting.

**spanning-tree [ mst *instance-id* ] port-priority *priority***

**no spanning-tree [ mst *instance-id* ] port-priority**

| Parameter<br>Description | Parameter                       | Description                                                                                                                                                |
|--------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <b>mst <i>instance-id</i></b>   | Instance ID, in the range from 0 to 63                                                                                                                     |
|                          | <b>priority <i>priority</i></b> | Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16. |

**Defaults** The default instance-id is 0.

The default priority is 128.

**Command** Interface configuration mode.

**Mode**

**Usage Guide** This command is MSTP-specific.

When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding.

Run this command to determine which port in the loop of a region enters the forwarding state.

**Configuration** This example sets the priority of gigabitethernet 0/1 to 10 in instance 20.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree mst 20 port-priority 0
```

| Related<br>Commands | Command                           | Description                                       |
|---------------------|-----------------------------------|---------------------------------------------------|
|                     | <b>show spanning-tree mst</b>     | Displays the MSTP information of an interface.    |
|                     | <b>spanning-tree mst cost</b>     | Sets the path cost.                               |
|                     | <b>spanning-tree mst priority</b> | Sets the device priority for different instances. |

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

## 10.29 spanning-tree priority

Use this command to set the device priority for different instances in the global configuration mode.

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

**spanning-tree [ mst *instance-id* ] priority *priority***

**no spanning-tree [ mst *instance-id* ] priority**

| Parameter<br>Description        | Parameter                                                                                                                                                                                      | Description                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
|                                 | <b>mst <i>instance-id</i></b>                                                                                                                                                                  | Instance ID, in the range from 0 to 63 |
| <b>priority <i>priority</i></b> | Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440, which are all multiples of 4096. |                                        |

**Defaults** The default instance ID is 0.  
The default device priority is 32768.

**Command Mode** Global configuration mode.

**Usage Guide** This command is MSTP-specific.  
Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

**Configuration Examples** The following example sets the device priority of the Instance to 8192.

```
Ruijie(config)# spanning-tree mst 20 priority 8192
```

| Related<br>Commands | Command                                | Description                                    |
|---------------------|----------------------------------------|------------------------------------------------|
|                     | <b>show spanning-tree mst</b>          | Displays the MSTP information of an interface. |
|                     | <b>spanning-tree mst cost</b>          | Sets path cost.                                |
|                     | <b>spanning-tree mst port-priority</b> | Sets the port priority of an instance.         |

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

### 10.30 spanning-tree pathcost method

Use this command to configure the path cost of the port. Use the **no** form of this command to restore the default setting.

**spanning-tree pathcost method { long | long standard | short }**

**no spanning-tree pathcost method**

| Parameter Description | Parameter            | Description                                                                                                                                                          |
|-----------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <b>long</b>          | Complies with the IEEE802.1t long with path cost ranging from 1 to 200,000,000.<br>Path cost of an aggregate port = 95% of the path cost of a physical port.         |
|                       | <b>long standard</b> | Complies with the IEEE802.1t long standard with path cost ranging from 1 to 200,000,000.<br>Path cost of an aggregate port = Path cost of a physical port/Linkupcnt. |
|                       | <b>short</b>         | Complies with the IEEE802.1d short with path cost ranging from 1 to 65,535.<br>Path cost of an aggregate port = 95% of the path cost of a physical port.             |

**Defaults** 802.1T standard is adopted to set path cost by default.

**Command** Global configuration mode.

**Mode**

**Usage Guide** If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

The following table lists path costs automatically configured for different link rate in three solutions.

| Port Rate | Port           | IEEE 802.1d Short | IEEE 802.1t Long | IEEE 802.1t Long Standard |
|-----------|----------------|-------------------|------------------|---------------------------|
| 10M       | Common port    | 100               | 2000000          | 2000000                   |
|           | Aggregate Port | 95                | 1900000          | 2000000/Linkupcnt         |
| 100M      | Common port    | 19                | 200000           | 200000                    |
|           | Aggregate Port | 18                | 190000           | 200000/Linkupcnt          |
| 1000M     | Common port    | 4                 | 20000            | 20000                     |
|           | Aggregate Port | 3                 | 19000            | 20000/Linkupcnt           |

|        |                |   |      |                 |
|--------|----------------|---|------|-----------------|
| 10000M | Common port    | 2 | 2000 | 2000            |
|        | Aggregate Port | 1 | 1900 | 20000/Linkupcnt |

When the long standard is used, the path cost of an aggregate port changes with the number of member ports in UP state, resulting in network topology change.

- If an aggregate port is static, linkupcnt in the table is the number of active member ports.
- If an aggregate port is an LACP aggregate port, linkupcnt in the table is the number of member ports forwarding aggregate port data.
- If no member port in the aggregate port goes UP, linkupcnt is 1.

**Configuration** The following example configures the path cost of the port.

**Examples**

```
Ruijie(config)# spanning-tree pathcost method long
```

**Related  
Commands**

| Command                             | Description                                      |
|-------------------------------------|--------------------------------------------------|
| <b>show spanning-tree interface</b> | Displays the STP configuration of the interface. |

**Platform** N/A

**Description**

## 10.31 spanning-tree portfast

Use this command to enable the portfast on the interface. Use the disabled form of this command to restore the default setting,

**spanning-tree portfast [ disabled ]**

**Parameter  
Description**

| Parameter       | Description                             |
|-----------------|-----------------------------------------|
| <b>disabled</b> | Disables the portfast on the interface. |

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide** After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.

**Configuration** The following example enables the portfast on the interface.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree portfast
```

| Related Commands | Command | Description                         |
|------------------|---------|-------------------------------------|
|                  |         | <b>show spanning-tree interface</b> |

Platform N/A  
Description

## 10.32 spanning-tree portfast bpdudfilter default

Use this command to enable the BPDU filter function globally. You can use the **no** form of the command to restore the default setting.

**spanning-tree portfast bpdudfilter default**

**no spanning-tree portfast bpdudfilter default**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       |           | N/A         |

Defaults This function is disabled by default,

Command Global configuration mode.  
Mode

Usage Guide The global BPDU filter function takes effect only when working with the PortFast function on the interface.  
Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the Port Fast interface. Use the **show spanning-tree** command to display the configuration.

Configuration The following example enables the BPDU filter function globally.

Examples 

```
Ruijie(config)# spanning-tree portfast bpdudfilter default
```

| Related Commands | Command | Description                         |
|------------------|---------|-------------------------------------|
|                  |         | <b>show spanning-tree interface</b> |

Platform N/A  
Description

## 10.33 spanning-tree portfast bpduguard default

Use this command to enable the BPDU guard globally. Use the **no** form of this command to restore the default setting,

**spanning-tree portfast bpduguard default**



**no spanning-tree portfast bpduguard default**


| Parameter<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          |           | N/A         |

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

**Command** Global configuration mode.

**Mode**

**Usage Guide** Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the **show spanning-tree** command to display the configuration.

 The global BPDU guard takes effect only when PortFast is enabled on a port.

**Configuration** The following example enables the GPDU guard globally.

**Examples** Ruijie(config)# spanning-tree portfast bpduguard default

| Related<br>Commands | Command | Description                         |
|---------------------|---------|-------------------------------------|
|                     |         | <b>show spanning-tree interface</b> |

**Platform** N/A

**Description**

## 10.34 spanning-tree portfast default

Use this command to enable the portfast feature on all interfaces globally. Use the **no** form of this command to restore the default setting.

**spanning-tree portfast default**

**no spanning-tree portfast default**

| Parameter<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          |           | N/A         |

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

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** The following example enables the portfast feature on all interfaces globally.

**Examples**

```
Ruijie(config)# spanning-tree portfast default
```

**Related  
Commands**

| Command                             | Description                            |
|-------------------------------------|----------------------------------------|
| <b>show spanning-tree interface</b> | Displays the global STP configuration. |

**Platform** N/A

**Description**

## 10.35 spanning-tree reset

Use this command to restore the **spanning-tree** configuration to the default setting.

**spanning-tree reset**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command  
Mode** Global configuration mode

**Usage Guide** The function do not have a **no** command.

**Configuration** The following example resets STP.

**Examples**

```
Ruijie(config)# spanning-tree reset
```

**Related  
Commands**

| Command                             | Description                                      |
|-------------------------------------|--------------------------------------------------|
| <b>show spanning-tree</b>           | Displays the global STP configuration.           |
| <b>show spanning-tree interface</b> | Displays the STP configuration of the interface. |

**Platform** N/A

**Description**

## 10.36 spanning-tree tc-guard

Use this command to enable **tc-guard** on the interface to prevent the spread of TC messages. Use the **no** form of this command to disable this function on the interface.

**spanning-tree tc-guard**

**no spanning-tree tc-guard**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

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

**Command Mode** Global configuration mode.

**Usage Guide** Enable TC guard to prevent TC packets from spreading

**Configuration Examples** The following example enables **tc-guard** on the interface Gi 0/1.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# spanning-tree tc-guard
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 10.37 spanning-tree tc-protection

Use this command to enable **tc-protection** globally. Use The **no** form of this command to disable this function.

**spanning-tree tc- protection**

**no spanning-tree tc- protection**

| 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 enables **tc-protection** globally.

```
Ruijie(config)# spanning-tree tc-protection
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 10.38 spanning-tree tc-protection tc-guard

Use this command to enable tc-guard to prevent TC packets from being flooded. Use the **no** form of this command to restore the default setting.

**spanning-tree tc-protection tc-guard**

**no spanning-tree tc-protection tc-guard**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

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

**Command Mode** Global configuration mode.

**Usage Guide** Enable TC guard to prevent TC packets from spreading.

**Configuration Examples** The following example enables tc-guard to prevent TC packets from being flooded.

```
Ruijie(config)# spanning-tree tc-protection tc-guard
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 10.39 spanning-tree tx-hold-count

Use this command to configure the TxHoldCount of the STP, the maximum number of the BPDU messages sent in one second. Use the **no** form of this command to restore the default setting.

**spanning-tree tx-hold-count *tx-hold-count***

**no spanning-tree tx-hold-count**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |                      |                                                                                                               |
|--------------------|----------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Description</b> |                      |                                                                                                               |
|                    | <i>tx-hold-count</i> | Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3. |

**Defaults** The default is 3.

**Command Mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example sets the maximum number of the BPDU messages sent in one second.

```
Ruijie(config)# spanning-tree tx-hold-count 5
```

|                         |                           |                                         |
|-------------------------|---------------------------|-----------------------------------------|
| <b>Related Commands</b> | <b>Command</b>            | <b>Description</b>                      |
|                         | <b>show spanning-tree</b> | Displays the global MSTP configuration. |

**Platform Description** N/A

## 11 LLDP Commands

### 11.1 civic-location

Use this command to configure a common LLDP address. Use the **no** form of this command to delete the 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
```

```
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. For example, the country code of China is CH. |
| <b>state</b>                           | Address information, CA type 1                                         |
| <b>county</b>                          | CA type 2                                                              |
| <b>city</b>                            | CA type 3                                                              |
| <b>division</b>                        | CA type 4                                                              |
| <b>neighborhood</b>                    | CA type 5                                                              |
| <b>street-group</b>                    | CA type 6                                                              |
| <b>leading-street-dir</b>              | CA type 16                                                             |
| <b>trailing-street-suffix</b>          | CA type 17                                                             |
| <b>street-suffix</b>                   | CA type 18                                                             |
| <b>number</b>                          | CA type 19                                                             |
| <b>street-number-suffix</b>            | CA type 20                                                             |
| <b>landmark</b>                        | CA type 21                                                             |
| <b>additional-location-information</b> | CA type 22                                                             |
| <b>name</b>                            | CA type 23                                                             |
| <b>postal-code</b>                     | CA type 24                                                             |
| <b>building</b>                        | CA type 25                                                             |
| <b>unit</b>                            | CA type 26                                                             |
| <b>floor</b>                           | CA type 27                                                             |
| <b>room</b>                            | CA type 28                                                             |
| <b>type-of-place</b>                   | CA type 29                                                             |
| <b>postal-community-name</b>           | CA type 30                                                             |
| <b>post-office-box</b>                 | CA type 31                                                             |

|                        |                     |
|------------------------|---------------------|
| <b>additional-code</b> | CA type 32          |
| <i>ca-word</i>         | Address information |

**Defaults** N/A

**Command Mode** LLDP Civic address configuration mode

**Usage Guide** To configure common LLDP address in LLDP civic address configuration mode, just enter the CA type key word and the *ca-word* parameter because the key word **civic-location** is unrecognized.

**Configuration** The following example configures an LLDP Civic Address (ID: 1).

**Examples**

```
Ruijie# config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
```

| Related Commands | Command                                                                                        | Description                                           |
|------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------|
|                  | <b>show lldp location civic-location { identifier id   interface interface-name   static }</b> | Displays the information about an LLDP Civic address. |

**Platform Description** N/A

## 11.2 clear lldp statistics

Use this command to clear LLDP statistics.

**clear lldp statistics [ interface interface-name ]**

| Parameter          | Parameter                       | Description    |
|--------------------|---------------------------------|----------------|
| <b>Description</b> | <b>interface interface-name</b> | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** **interface** parameter: clear the LLDP statistics of the specified interface

**Configuration** The following example clears LLDP statistics of interface 1.

**Examples**

```
Ruijie# clear lldp statistics interface GigabitEthernet 0/1
Ruijie# 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  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

Platform N/A

Description

### 11.3 clear lldp table

Use this command to clear LLDP neighbor information.

**clear lldp table** [ interface *interface-name* ]

| Parameter   | Parameter                       | Description    |
|-------------|---------------------------------|----------------|
| Description | interface <i>interface-name</i> | Interface name |

Defaults N/A

Command Privileged EXEC mode  
Mode

**Usage Guide** If the **interface** parameter is specified, the LLDP neighbor information on the specified interface is cleared.  
If the **interface** 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 Ruijie# 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
Ruijie# clear lldp table interface GigabitEthernet 0/1
Ruijie# show lldp neighbors interface GigabitEthernet 0/1
```

| Related | Command | Description |
|---------|---------|-------------|
|---------|---------|-------------|



|                 |     |     |
|-----------------|-----|-----|
| <b>Commands</b> | N/A | N/A |
|-----------------|-----|-----|

**Platform** N/A

**Description**

## 11.4 device-type

Use this command to configure the device type. Use the **no** or **default** form of this command to restore the default setting.

**device-type** *device-type*

**no device-type**

**default device-type**

| Parameter          | Parameter          | Description                                                                                                                                                   |
|--------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <i>device-type</i> | Device type. The value ranges from 0 to 2.<br>0: The device type is DHCP Server.<br>1: The device type is switch.<br>2: The device type is LLDP MED terminal. |

**Defaults**

**Command** LLDP Civic address configuration mode

**Mode**

**Usage Guide** This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.

**Configuration** The following example sets the device type to switch.

**Examples**

```
Ruijie# config
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# device-type 1
```

| Related         | Command                                                                                                      | Description                              |
|-----------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <b>Commands</b> | <b>show lldp location civic-location { identifier <i>id</i>   interface <i>interface-name</i>   static }</b> | Displays LLDP Civic Address information. |

**Platform** N/A

**Description**

## 11.5 lldp enable

Use this command to enable the LLDP globally or on the interface. Use **no** or **default** form of this command to disable this function.

**lldp enable**  
**no lldp enable**  
**default lldp enable**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

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

**Command Mode** Global (or 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.

```
Ruijie# config
Ruijie(config)# no lldp enable
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no lldp enable
```

| Related Commands | Command                 | Description                       |
|------------------|-------------------------|-----------------------------------|
|                  | <b>show lldp status</b> | Displays LLDP status information. |

**Platform Description** N/A

## 11.6 lldp encapsulation snap

Use this command to configure the encapsulation format of LLDP packets. Use the **no** or **default** form of this command to restore the default setting.

**lldp encapsulation snap**  
**no lldp encapsulation snap**  
**default lldp encapsulation snap**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** By default, Ethernet II encapsulation format is used.

**Command Mode** Interface configuration 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**

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp encapsulation snap
```

**Related****Commands**

| Command          | Description                       |
|------------------|-----------------------------------|
| show lldp status | Displays LLDP status information. |

**Platform**

N/A

**Description**

## 11.7 lldp error-detect

Use this command to configure the LLDP error detection, including the detection of VLAN configurations on both sides of the link, port state detection, port aggregation configuration detection, MTU configuration detection and loop detection. If any error is detected by LLDP, warning message will be printed to notify the administrator. Use the **no** or **default** form of this command to disable this function.

**lldp error-detect**

**no lldp error-detect**

**default lldp error-detect**

**Parameter****Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults**

This function is enabled by default.

**Command**

Interface configuration mode.

**Mode****Usage Guide**

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**

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp error-detect
```

**Related**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                 |                              |                                   |
|-----------------|------------------------------|-----------------------------------|
| <b>Commands</b> | <b>show interface status</b> | Displays LLDP status information. |
|-----------------|------------------------------|-----------------------------------|

**Platform** N/A

**Description**

## 11.8 lldp fast-count

When a new neighbor is detected or when LLDP operating mode changes from shutdown or Rx to TxRx or Tx, to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism shortens the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs before restoring to the normal transmit interval. Use the **no** or **default** form of this command to restore the default setting.

**lldp fast-count** *value*

**no lldp fast-count**

**default lldp fast-count**

| Parameter          | Parameter    | Description                                                      |
|--------------------|--------------|------------------------------------------------------------------|
| <b>Description</b> | <i>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** N/A

**Configuration Examples** The following example sets the number of fast sent LLDP packets to 5.

```
Ruijie# config
Ruijie(config)# lldp fast-count 5
```

| Related Commands | Command                      | Description                       |
|------------------|------------------------------|-----------------------------------|
|                  | <b>show interface status</b> | Displays LLDP status information. |

**Platform** N/A

**Description**

## 11.9 lldp hold-multiplier

Use this command to set the TTL multiplier. Use the **no** or **default** form of this command to restore to default setting.

**lldp hold-multiplier** *value*

**no lldp hold-multiplier**

**default lldp hold-multiplier**

| Parameter                     | Parameter                                                                                                                                                                                                                 | Description                                |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <b>Description</b>            | <i>value</i>                                                                                                                                                                                                              | TTL multiplier, in the range from 2 to 10. |
| <b>Defaults</b>               | The default is 4.                                                                                                                                                                                                         |                                            |
| <b>Command Mode</b>           | Global configuration mode.                                                                                                                                                                                                |                                            |
| <b>Usage Guide</b>            | 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. |                                            |
| <b>Configuration Examples</b> | The following example sets TTL multiplier to 5.                                                                                                                                                                           |                                            |
|                               | <pre>Ruijie# config Ruijie(config)# lldp hold-multiplier 5</pre>                                                                                                                                                          |                                            |
| Related Commands              | Command                                                                                                                                                                                                                   | Description                                |
|                               | <b>show lldp status</b>                                                                                                                                                                                                   | Displays LLDP status information.          |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                       |                                            |

## 11.10 lldp location civic-location identifier

Use this command to create a common address of a device connected to the network in LLDP Civic Address configuration mode. Use the **no** or **default** form of this command to delete the address.

**lldp location civic-location identifier *id***  
**no lldp location civic-location identifier *id***  
**default lldp location civic-location identifier *id***

| Parameter                     | Parameter                                                                                                   | Description                                                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Description</b>            | <i>id</i>                                                                                                   | ID of a common address of a network device, in the range from 1 to 1024. |
| <b>Defaults</b>               | N/A                                                                                                         |                                                                          |
| <b>Command Mode</b>           | Global configuration mode                                                                                   |                                                                          |
| <b>Usage Guide</b>            | This command can be used to enter the LLDP Civic Address configuration mode.                                |                                                                          |
| <b>Configuration Examples</b> | The following example creates the Civic Address information in LLDP MED-TLV as follows: set <i>id</i> to 1. |                                                                          |
|                               | <pre>Ruijie# config</pre>                                                                                   |                                                                          |

```
Ruijie(config)# lldp location civic-location identifier 1
Ruijie(config-lldp-civic)#
```

| Related Commands | Command                                                                                                                           | Description                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
|                  | <b>show lldp location civic-location</b> { <b>identifier</b> <i>id</i>   <b>interface</b> <i>interface-name</i>   <b>static</b> } | Displays the LLDP Civic Address information. |

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

## 11.11 lldp location elin identifier

Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the **no** or **default** form of this command to delete the number.

**lldp location elin identifier** *id* **elin-location** *tel-number*

**no lldp location elin identifier** *id*

**default lldp location elin identifier** *id*

| Parameter Description | Parameter                              | Description                                             |
|-----------------------|----------------------------------------|---------------------------------------------------------|
|                       | <b>identifier</b> <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** N/A

**Command Mode** Global configuration mode

**Usage Guide** This command is used to configure an emergency number.

**Configuration Examples** The following example sets an emergency number.

```
Ruijie# config
Ruijie(config)# lldp location elin identifier 1 elin-location 085283671111
```

| Related Commands | Command                                                                                                                          | Description                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
|                  | <b>show lldp location elin-location</b> { <b>identifier</b> <i>id</i>   <b>interface</b> <i>interface-name</i>   <b>static</b> } | Displays an LLDP emergency number. |

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

## 11.12 lldp management-address-tlv

Use this command to configure the management address advertised in LLDP packets. Use the **no** or

**default** form of this command to disable the advertisement of management address.

**lldp management-address-tlv** [ *ip-address* ]

**no lldp management-address-tlv**

**default lldp management-address-tlv**

| Parameter   | Parameter         | Description                                        |
|-------------|-------------------|----------------------------------------------------|
| Description | <i>ip-address</i> | The management address advertised in LLDP packets. |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** By default, the management address is advertised in LLDP packets, and is the IPv4 address of the lowest-ID VLAN carried on the port. If IPv4 address is not configured for this VLAN, the next lowest-ID VLAN carried on the port will be tried until the IPv4 address is obtained.

**Configuration Examples** The following example configures the management address advertised in LLDP packets to 192.168.1.1.

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp management-address-tlv
192.168.1.1
```

| Related Commands | Command                            | Description                     |
|------------------|------------------------------------|---------------------------------|
|                  | <b>show lldp local-information</b> | Displays LLDP local information |

**Platform Description** N/A

## 11.13 lldp mode

Use this command to configure the LLDP operating mode. Use **no** or **default** form of this command to restore the default setting.

**lldp mode** { *rx* | *tx* | *txrx* }

**no lldp mode**

**default lldp mode**

| Parameter   | Parameter   | Description                 |
|-------------|-------------|-----------------------------|
| Description | <b>rx</b>   | Only sends LLDPDUs.         |
|             | <b>tx</b>   | Only receives LLDPDUs.      |
|             | <b>txrx</b> | Sends and receives LLDPDUs. |

- Defaults** The default is **txrx**.
- 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.

**Examples**

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp mode tx
```

| Related Commands | Command                 | Description                      |
|------------------|-------------------------|----------------------------------|
|                  | <b>show lldp status</b> | Displays LLDP status information |

**Platform** N/A

**Description**

## 11.14 lldp network-policy profile

Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the **no** or **default** form of this command to delete the policy.

**lldp network-policy profile** *profile-num*  
**no lldp network-policy profile** *profile-num*  
**default lldp network-policy profile** *profile-num*

| Parameter          | Parameter          | Description                                                |
|--------------------|--------------------|------------------------------------------------------------|
| <b>Description</b> | <i>profile-num</i> | ID of an LLDP network policy, in the range from 1 to 1024. |

**Defaults** N/A

**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 Examples** The following example creates an LLDP network policy whose ID is 1.

**Examples**

```
Ruijie# config
```



```
Ruijie(config)# lldp network-policy profile 1
Ruijie(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**

## 11.15 lldp notification remote-change enable

Use this command to configure LLDP Trap. Use the **no** or **default** form of this command to restore the default setting.

**lldp notification remote-change enable**

**no lldp notification remote-change enable**

**default lldp notification remote-change enable**

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

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

**Command** Interface configuration mode.

**Mode**

**Usage Guide** By configuring LLDP Trap, 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.

**Examples**

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp notification remote-change enable
```

| Related Commands | Command                 | Description                       |
|------------------|-------------------------|-----------------------------------|
|                  | <b>show lldp status</b> | Displays LLDP status information. |

**Platform** N/A

**Description**

## 11.16 lldp timer notification-interval

Use this command to set an interval of sending LLDP Traps. Use the **no** or **default** form of this command to restore the default setting.

**lldp timer notification-interval** *seconds*

**no lldp timer notification-interval**

**default lldp timer notification-interval**

| Parameter   | Parameter      | Description                                                                         |
|-------------|----------------|-------------------------------------------------------------------------------------|
| Description | <i>seconds</i> | Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds. |

**Defaults** The default is 5s.

**Command Mode** Global configuration mode.

**Usage Guide** To prevent excessive LLDP traps from being sent, you can set an interval of sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.

**Configuration Examples** The following example sets the interval of sending LLDP Traps to 10 seconds.

```
Ruijie# config
Ruijie(config)# lldp timer notification-interval 10
```

| Related Commands | Command                 | Description                       |
|------------------|-------------------------|-----------------------------------|
|                  | <b>show lldp status</b> | Displays LLDP status information. |

**Platform Description** N/A

## 11.17 lldp timer reinit-delay

Use this command to set port initialization delay. Use the **no** or **default** form of this command to restore the default setting.

**lldp timer reinit-delay** *seconds*

**no lldp timer reinit-delay**

**default lldp timer reinit-delay**

| Parameter   | Parameter      | Description                                                                  |
|-------------|----------------|------------------------------------------------------------------------------|
| Description | <i>seconds</i> | Port initialization delay, in the range from 1 to 10 in the unit of seconds. |

- Defaults** The default 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.

```
Ruijie# config
Ruijie(config)# lldp timer reinit-delay 3
```

| Related Commands | Command                 | Description                       |
|------------------|-------------------------|-----------------------------------|
|                  | <b>show lldp status</b> | Displays LLDP status information. |

**Platform Description** N/A

## 11.18 lldp timer tx-delay

Use this command to set LLDP packet transmission delay. Use the **no** or **default** form of this command to restore the default setting.

**lldp timer tx-delay** *seconds*

**no lldp timer tx-delay**

**default lldp timer tx-delay**

| Parameter Description | Parameter      | Description                                                                         |
|-----------------------|----------------|-------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds. |

- Defaults** The default 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.

```
Ruijie# config
Ruijie(config)# lldp timer tx-delay 3
```

| Related  | Command                 | Description                       |
|----------|-------------------------|-----------------------------------|
| Commands | <b>show lldp status</b> | Displays LLDP status information. |

Platform N/A  
Description

## 11.19 lldp timer tx-interval

Use this command to set the interval of sending the LLDP packets. Use **no** or **default** form of this command to restore the default setting.

**lldp timer tx-interval** *seconds*

**no lldp timer tx-interval**

**default lldp timer tx-interval**

| Parameter   | Parameter      | Description                                                                                |
|-------------|----------------|--------------------------------------------------------------------------------------------|
| Description | <i>seconds</i> | Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds. |

Defaults The default 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

```
Ruijie# config
Ruijie(config)# lldp timer tx-interval 10
```

| Related  | Command                 | Description                       |
|----------|-------------------------|-----------------------------------|
| Commands | <b>show lldp status</b> | Displays LLDP status information. |

Platform N/A  
Description

## 11.20 lldp tlv-enable

Use this command to configure the types of advertisable TLVs. Use the **no** or **default** form of this command to restore the default setting.

**lldp tlv-enable** *tlv-type subtype*

**no lldp tlv-enable** *tlv-type subtype*  
**default lldp tlv-enable** *tlv-type subtype*

**Parameter** Parameter *tlv-type* includes **basic-tlv**, **dot1-tlv**, **dot3-tlv** and **med-tlv**.  
**Description** The *subtype* parameter depends on the *tlv-type*.

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>basic-tlv</b> | Basic management TLVs: <ul style="list-style-type: none"> <li>● <b>all</b>: All basic TLVs.</li> <li>● <b>port-description</b>: Port Description TLV.</li> <li>● <b>system-capability</b>: System Capabilities TLV.</li> <li>● <b>system-description</b>: System Description TLV.</li> <li>● <b>system-name</b>: System Name TLV.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>dot1-tlv</b>  | 802.1 organizationally specific TLVs: <ul style="list-style-type: none"> <li>● <b>all</b>: All dot1 TLV.</li> <li>● <b>port-vlan-id</b>: Port VLAN ID TLV.</li> <li>● <b>protocol-vlan-id</b> [ <i>vlan-id</i> ] : Port And Protocol VLAN ID TLV.</li> <li>● <b>vlan-name</b> [ <i>vlan-id</i> ] : VLAN Name TLV.</li> </ul> <i>vlan-id</i> : Indicates the VLAN name, ranging from 1 to 4,094.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>dot3-tlv</b>  | 802.3 organizationally specific TLV: <ul style="list-style-type: none"> <li>● <b>all</b>: All dot3 TLV.</li> <li>● <b>link-aggregation</b>: Link Aggregation TLV.</li> <li>● <b>mac-physic</b>: MAC/PHY Configuration/Status TLV.</li> <li>● <b>max-frame-size</b>: Maximum Frame Size TLV.</li> <li>● <b>power</b>: Power Via MDI TLV.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>med-tlv</b>   | LLDP MED TLV: <ul style="list-style-type: none"> <li>● <b>all</b>: All MED TLVs.</li> <li>● <b>capability</b>: LLDP-MED Capabilities TLV.</li> <li>● <b>inventory</b>:<br/>Inventory management TLVs, which contains the hardware version, firmware version, software version, SN, manufacturer name, module name, and asset identifier.</li> <li>● <b>location</b> { <b>civic-location</b>   <b>elin</b> } <b>identifier</b> <i>id</i>: Location Identification TLV; <b>civic-location</b>: Indicates the civic address information and postal information. <b>elin</b>: Indicates the emergency telephone number; <i>id</i>: Indicates the policy ID, ranging from 1 to 1,024.</li> <li>● <b>network-policy profile</b> [ <i>profile-num</i> ]:<br/>Network Policy TLV, <i>profile-num</i>: Indicates the Network Policy ID, ranging from 1 to 1,024.</li> <li>● <b>power-over-ethernet</b>: Extended Power-via-MDI TLV.</li> </ul> |

**Defaults** By default, all TLVs other than Location Identification TLV can be advertised on the interface for products other than S12000. For the S12000 product series, only basic TLVs and IEEE 802.1 TLVs are advertised. To advertise IEEE 802.3 TLVs and LLDP-MED TLVs, run the **lldp tlv-enable** command.

**Command** Interface configuration mode

**Mode**

**Usage Guide** During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the **all** parameter is specified, all optional TLVs of the types are advertised.

During configuration of LLDP-MED TLVs, if the **all** parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised.

When configuring LLDP-MED Capability TLVs, configure LLDP-MED MAC/PHY TLVs first. When canceling LLDP-MED MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first.

When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured.

To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED Capability TLVs can be canceled.

**Configuration** The following example configures all IEEE 802.1 TLVs to be advertised.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable dot1-tlv all
```

The following example applies LLDP network policy 1 on the 0/1 interface.

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy
profile 1
```

The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface.

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv location
civic-location identifier 1
```

The following example applies the emergency number (ID: 1) on the 0/1 interface.

```
Ruijie# config
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp location elin identifier 1
```

| Related         | Command                               | Description                                  |
|-----------------|---------------------------------------|----------------------------------------------|
| <b>Commands</b> | <b>show lldp tlv-config interface</b> | Displays the attributes of advertisable TLVs |

**Platform** N/A

**Description**

## 11.21 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-name* ]

| Parameter   | Parameter                              | Description                                    |
|-------------|----------------------------------------|------------------------------------------------|
| Description | <b>global</b>                          | Displays the global LLDP information.          |
|             | <b>interface</b> <i>interface-name</i> | Displays the interface-based LLDP information. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If no parameter is specified, all LLDP information, including global and interface-based LLDP information, will be displayed.

**Configuration Examples** The following example displays the device information to be sent to neighbor device.

```
Ruijie# 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.<br>Network connectivity device<br>Class I: normal terminal device<br>Class II: media terminal device; besides Class I capabilities, it also supports media streams.<br>Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication. |
| 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                                                                                                                                                                                                                                                                                                                                                  |
| PPVID Enabled                   | Indicates whether port and protocol VLAN is enabled                                                                                                                                                                                                                                                                                                                                                    |
| VLAN name of VLAN 1             | Name of VLAN 1                                                                                                                                                                                                                                                                                                                                                                                         |
| Protocol Identity               | Protocol identifier                                                                                                                                                                                                                                                                                                                                                                                    |
| Auto-negotiation supported      | Indicates whether auto-negotiation is supported                                                                                                                                                                                                                                                                                                                                                        |
| Auto-negotiation enabled        | Indicates whether auto-negotiation is enabled                                                                                                                                                                                                                                                                                                                                                          |
| 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                                                                                                                                                                                                                                                                                                                                                                     |
| Link aggregation supported      | Indicates whether link aggregation is supported                                                                                                                                                                                                                                                                                                                                                        |
| Link aggregation enabled        | Indicates whether link aggregation is enabled                                                                                                                                                                                                                                                                                                                                                          |
| 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:<br>PSE (power sourcing equipment)<br>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** N/A

**Description**

## 11.22 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-name* | **static** }

| Parameter Description | Parameter                              | 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.<br><i>id</i> is the policy ID, in the range from 1 to 1024. |
|                       | <b>Interface</b> <i>interface-name</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** Privileged 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
Ruijie# 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.

```

Ruijie# show lldp location elin-location static
Elin location information

Identifier : t
Elin : iiiiixixixi
Ports : Gi0/1

```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

Platform N/A

Description

### 11.23 show lldp neighbors

Use this command to display the LLDP information about a neighboring device.

**show lldp neighbors** [ **interface** *interface-name* ] [ **detail** ]

| Parameter   | Parameter                              | Description                                |
|-------------|----------------------------------------|--------------------------------------------|
| Description | <b>interface</b> <i>interface-name</i> | Interface name                             |
|             | <b>detail</b>                          | All information about a neighboring device |

Defaults N/A

Command Privileged EXEC mode  
 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** parameter is specified, the neighboring device information received on the specified interface is displayed.

**Configuration** The following example displays the neighboring device information received on all ports.

**Examples**

```
Ruijie# 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 :

```

| 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<br>Network connectivity device:<br>Class I: general terminal device<br>Class II: media terminal device, including capabilities of Class I and supporting media stream<br>Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication |
| 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**

## 11.24 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-name* }

| Parameter          | Parameter                              | Description                                                                                                                                                      |
|--------------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> |                                        | Displays all LLDP network policies if no <i>profile-num</i> is specified.                                                                                        |
|                    | <b>profile</b> [ <i>profile-num</i> ]  | Displays the specified LLDP network policy if a <i>profile-num</i> is configured. <i>profile-num</i> is the ID of a network policy, in the range from 1 to 1024. |
|                    | <b>interface</b> <i>interface-name</i> | Displays the LLDP network policy of the specified interface.                                                                                                     |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** If *profile-num* 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 Examples** The following example displays the information about a network policy.

```
Ruijie#
show lldp network-policy profile
network-policy information:

Network Policy Profile 1
 voice vlan 2 cos 4 dscp 6
 voice-signaling vlan 2000 cos 4 dscp 6
```

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

**Platform** N/A

**Description**

## 11.25 show lldp statistics

The following example displays LLDP statistics.

**show lldp statistics** [ **global** | **interface** *interface-name* ]

| Parameter   | Parameter                              | Description                                              |
|-------------|----------------------------------------|----------------------------------------------------------|
| Description | <b>global</b>                          | Displays the global LLDP statistics.                     |
|             | <b>interface</b> <i>interface-name</i> | Displays the LLDP statistics of the specified interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration Examples** The following example displays all LLDP statistics.

```
Ruijie# 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
```

| 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**

## 11.26 show lldp status

Use this command to display LLDP status information.

**show lldp status** [ **interface** *interface-name* ]

| Parameter          | Parameter                              | Description                                                      |
|--------------------|----------------------------------------|------------------------------------------------------------------|
| <b>Description</b> | <b>interface</b> <i>interface-name</i> | Displays the LLDP status information of the specified interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** If no parameter is specified, LLDP status information of all interfaces will be displayed.

**Configuration Examples** The following example displays LLDP status information of all ports.

```
Ruijie# 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

```

| 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 Traps                 |
| 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 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**

### 11.27 show lldp tlv-config

Use this command to display the advertisable TLV configuration of a port.

**show lldp tlv-config** [ **interface** *interface-name* ]

| Parameter          | Parameter                              | Description                                                     |
|--------------------|----------------------------------------|-----------------------------------------------------------------|
| <b>Description</b> | <b>interface</b> <i>interface-name</i> | Displays the LLDP TLV configuration of the specified interface. |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** If no parameter is specified, the LLDP TLV configuration of all interfaces will be displayed.

**Configuration** The following example displays TLV information of port 1.

**Examples**

```
Ruijie# 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**

**Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 11.28 voice vlan

Use this command to configure the LLDP network policy. Use the **no** or **default** form of this command to delete the policy.

```
{ voice | voice-signaling } vlan { vlan-id | dot1p } [cos cvalue | dscp dvalue]
```

```
{ voice | voice-signaling } vlan untagged
```

```
{ voice | voice-signaling } vlan none
```

```
no { voice | voice-signaling } vlan
```

```
default { voice | voice-signaling } vlan
```

| Parameter   | Parameter              | Description                                                                                                                                     |
|-------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <b>voice</b>           | Voice application                                                                                                                               |
|             | <b>voice-signaling</b> | Voice-signaling application                                                                                                                     |
|             | <i>vlan-id</i>         | (Optional) VLAN ID of voice flow. The value ranges from 1 to 4094.                                                                              |
|             | <b>dot1p</b>           | (Optional) The 802.1p priority frame, which is able to carry CoS and DSCP values and is tagged with CoS priority and VLAN ID of 0.              |
|             | <b>cos cvalue</b>      | (Optional) Class of service .CoS of the configured voice flow. The value ranges from 0 to 7, and the default value is 5.                        |
|             | <b>dscp dvalue</b>     | (Optional) Differentiated services code point. DSCP value of the configured voice flow. The value ranges from 0 to 63. The default value is 46. |
|             | <b>untagged</b>        | (Optional) The untagged frame, which does not carry VLAN ID or CoS priority.                                                                    |
|             | <b>none</b>            | (Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration.                                 |

**Defaults** N/A

**Command** LLDP network policy configuration mode

**Mode**

**Usage Guide** In the LLDP network policy configuration mode, configure the LLDP network policy.

Voice indicates the voice data type, and voice-signaling indicates the voice signal type.

If a device connects to an IP phone and the IP phone supports LLDP-MED, the network policy TLV can be configured to deliver policies to the IP phone, so that the IP phone changes the voice stream tag and QoS. Excluding the preceding policy, the following operations need to be performed on the device:

1. Enable the voice VLAN function and add the port connected to the IP phone to the voice VLAN in static mode.
2. Configure the port connected to the IP phone to a QoS trusted port. (It is recommended to use the trusted DSCP mode.)
3. If 802.1X authentication is enabled on the port at the same time, a security channel needs to be configured to transmit packets from the voice VLAN.

If the IP phone does not support LLDP-MED, the voice VLAN function must be enabled. In addition, the MAC address of the IP phone needs to be added to the voice VLAN OUI list manually.

For details about how to configure the QoS trusted mode, see chapter "IP QoS." For details about how to configure the voice VLAN, see chapter "Voice VLAN." For details about how to configure the security channel, see chapter "ACL."

**Configuration** The following example configures the LLDP network policy (profile-num is 1).

**Examples**

```
Ruijie# config
Ruijie(config)# lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan untagged
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6
```

**Related**

**Commands**

| Command                                                        | Description                       |
|----------------------------------------------------------------|-----------------------------------|
| <b>show lldp network-policy profile</b> [ <i>profile-num</i> ] | Displays the LLDP network policy. |

**Platform**

N/A

**Description**

## IP Address & Application Commands

---

1. IP Address/Service Commands
2. ARP Commands
3. DHCP Commands
4. DNS Commands
5. Network Connectivity Test Tool Commands
6. TCP Commands
7. IPv4 REF Commands

# 1 IP Address/Service 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. |
|                       | <b>secondary</b>    | Secondary IP address                                                                                                                                 |

**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 IP 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 .

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 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 broadcast-address

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-address** *ip-address*

**no ip broadcast-address**

| Parameter          | Parameter         | Description                     |
|--------------------|-------------------|---------------------------------|
| <b>Description</b> | <i>ip-address</i> | Broadcast address of IP network |

**Defaults** The default IP broadcast address is 255.255.255.255.

**Command Mode** Interface configuration 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.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# ip broadcast-address 0.0.0.0
```



| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

### 1.3 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.<br>The default is 100. |
|                       | <i>bucket-size</i>  | The number of tokens in the bucket, in the range is from 1 to 200.<br>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.

```
Ruijie(config)# ip icmp error-interval DF 1000 100
```

The following example sets the rate to send other ICMP error packets to 10 per second.

```
Ruijie(config)# ip icmp error-interval 1000 10
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.4 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**

| Parameter          | Parameter | Description |
|--------------------|-----------|-------------|
| <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**

```
Ruijie(config)# no ip source-route
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.5 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   | Parameter    | Description                                                           |
|-------------|--------------|-----------------------------------------------------------------------|
| 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** Ruijie(config)# ip ttl 100

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.6 show ip interface

Use this command to display the IP status information of an interface.

**show ip interface** [ *interface-type interface-number* | **brief** ]

| Parameter   | Parameter               | Description                                                                                                                                     |
|-------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <i>interface-type</i>   | Specifies interface type.                                                                                                                       |
|             | <i>interface-number</i> | Specifies interface number.                                                                                                                     |
|             | <b>brief</b>            | 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**

```
Ruijie#show ip interface brief
Interface IP-Address (Pri) IP-Address (Sec) Status Protocol
Loopback 2 no address no address up down
VLAN 1 no address no address down down
VLAN 2 no address no address down down
```

| 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.

```
Ruijie#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

| 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:<br>0<br>Request packet:<br>0<br>Reply packet:<br>0<br>Unknown packet:<br>0                          | Show the total number of ARP packets received on the interface, including:<br>ARP request packet<br>ARP reply packet<br>Unknown packet                                                              |
| TTL invalid packet number:                                                                                                   | Show the TTL invalid packet number                                                                                                                                                                  |
| ICMP packet input number: 0<br>Echo request: 0<br>Echo reply: 0<br>Unreachable: 0<br>Source quench: 0<br>Routing redirect: 0 | Show the total number of ICMP packets received on the interface, including:<br>Echo request packet<br>Echo reply packet<br>Unreachable packet<br>Source quench packet<br>Routing redirection packet |

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.7 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                                   |
|                    | <b>total</b>          | 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**

```

R1#show ip packet statistics
Total
 Received 113962 packets, 11948991 bytes
 Unicast:90962,Multicast:5232,Broadcast:17768
 Discards:0
 HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
 NoRoutes:0
 Others:0
 Sent 34917 packets, 1863146 bytes
 Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
 Received 6715 packets, 416587 bytes
 Unicast:2482,Multicast:4233,Broadcast:0
 Discards:0
 HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)
 NoRoutes:0
 Others:0
 Sent 6720 packets, 417096 bytes
 Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
 Received 0 packets, 0 bytes
 Unicast:0,Multicast:0,Broadcast:0
 Discards:0
 HdrErrors:0 (BadChecksum:0,TTLExceeded:0,Others:0)

```

```
NoRoutes:0
Others:0
Sent 0 packets, 0 bytes
Unicast:0,Multicast:0,Broadcast:0
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.8 show ip raw-socket

Use this command to display IPv4 raw sockets.

**show ip raw-socket** [ *num* ]

| Parameter          | Parameter  | Description |
|--------------------|------------|-------------|
| <b>Description</b> | <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**

```
Ruijie# 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  |
|--------------|--------------|
| Number       | Number       |
| Protocol     | Protocol     |
| Process name | Process name |
| Total        | Total number |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 1.9 show ip sockets

Use this command to display all IPv4 sockets.

**show ip sockets**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The following displays all IPv4 sockets.

### Examples

```
Ruijie# show ip sockets
Number Process name Type Protocol LocalIP:Port
ForeignIP:Port State
1 dhcpc.elf DGRAM UDP 0.0.0.0:68 0.0.0.0:0
*
2 ntp.elf DGRAM UDP 0.0.0.0:123 0.0.0.0:0
*
3 rg-snmpd DGRAM UDP 0.0.0.0:161 0.0.0.0:0
*
4 ntp.elf DGRAM UDP 0.0.0.0:1230 0.0.0.0:0
*
5 rg-snmpd DGRAM UDP 0.0.0.0:51602 0.0.0.0:0
*
6 rg-telnetd STREAM TCP 0.0.0.0:23 0.0.0.0:0
LISTEN
7 httpd.elf STREAM TCP 0.0.0.0:80 0.0.0.0:0
LISTEN
8 httpd.elf STREAM TCP 0.0.0.0:443 0.0.0.0:0
LISTEN
9 cwmp_gsoap.elf STREAM TCP 0.0.0.0:7547 0.0.0.0:0
LISTEN
10 rg-telnetd STREAM TCP 172.18.23.245:23
172.16.116.235:57359 ESTABLISHED
11 rg-telnetd STREAM TCP 172.18.23.245:23
172.16.117.148:50955 ESTABLISHED
```



```
12 rg-telnetd STREAM TCP 172.18.23.245:23
Total: 12
```

| Field          | Description                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| Number         | Serial number.                                                                                                  |
| Process name   | Process name.                                                                                                   |
| Type           | Socket type, including the following types:<br>RAW: raw sockets<br>DGRAM: datagram type<br>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** N/A

**Description**

## 1.10 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          | Parameter             | Description       |
|--------------------|-----------------------|-------------------|
| <b>Description</b> | <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**

```
Ruijie# show ip udp
Number Local Address Peer Address Process name
```

|   |               |           |           |
|---|---------------|-----------|-----------|
| 1 | 0.0.0.0:68    | 0.0.0.0:0 | dhcpc.elf |
| 2 | 0.0.0.0:123   | 0.0.0.0:0 | ntp.elf   |
| 3 | 0.0.0.0:161   | 0.0.0.0:0 | rg-snmpd  |
| 4 | 0.0.0.0:51602 | 0.0.0.0:0 | rg-snmpd  |

| 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** N/A

**Description**

## 2 ARP Commands

### 2.1 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 MAC-address type*

| 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.

**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**

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

| Related  | Command         | Description                |
|----------|-----------------|----------------------------|
| Commands | clear arp-cache | Clears the ARP cache table |

**Platform** N/A

**Description**

### 2.2 arp anti-ip-attack

For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learning). Sending large number of this message to the CPU will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messages with that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address

in hardware.

In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possible to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the *num* parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function. Use the **arp anti-ip-attack** command to set the parameter or disable this function. Use the **no** form of this command to restore the default setting.

**arp anti-ip-attack num**  
**no arp anti-ip-attack**

| Parameter Description | Parameter  | Description                                                                                                                                            |
|-----------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>num</i> | The number of the IP message to trigger the ARP to discarded entry in the range from 0 to 100. 0 stands for disabling the arp anti-ip-attack function. |

**Defaults** By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.

**Command Mode** Global configuration mode.

**Usage Guide** The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the **arp anti-ip-attack num** could be smaller. If not, in order to preferential ensure the use of the normal routing, the *num* could be larger or disable this function.

**Configuration Examples** The following example sets the IP message number that triggers ARP to discarding entry as 5.

```
Ruijie(config)# arp anti-ip-attack 5
```

The following example disables the ARP anti-ip-attack function.

```
Ruijie(config)# arp anti-ip-attack 0
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 2.3 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

**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** The following example sets the maximum number of ARP learned on the interface to 300.

**Examples**

```
Ruijie(config)# interface vlan1
Ruijie(config-if- VLAN 1)# arp cache interface-limit 300
```

The following example restores the default setting.

```
Ruijie(config)# interface vlan1
Ruijie(config-if- VLAN 1)# no arp cache interface-limit
```

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

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

## 2.4 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**

| <b>Parameter Description</b> | <b>Parameter</b> | <b>Description</b>                                                                                           |
|------------------------------|------------------|--------------------------------------------------------------------------------------------------------------|
|                              | <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 gratuitous ARP requests that are sent. The default value is 1. The value ranges from 1 to 100. |

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

**Command Mode** Interface configuration mode.

**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** The following example sets to send one free ARP request to SVI 1 per second.

**Examples**

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# arp gratuitous-send interval 1
```

The following example stops sending the free ARP request to SVI 1.

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)# no arp gratuitous-send
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 2.5 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****Description**

| Parameter      | 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.

**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.

```
Ruijie(config)# arp retry interval 30
```

**Related****Commands**

| Command                | Description                                                |
|------------------------|------------------------------------------------------------|
| <b>arp retry times</b> | Number of times for retransmitting an ARP request message. |

**Platform**

N/A

**Description**

## 2.6 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. |

**Defaults** The default is 5.

**Command Mode** Global configuration mode.

**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 Examples** The following example sets the local ARP request not to be retried.

```
Ruijie(config)# arp retry times 1
```

The following example sets the local ARP request to be retried for one time.

```
Ruijie(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**

## 2.7 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   | Parameter      | Description                                                           |
|-------------|----------------|-----------------------------------------------------------------------|
| 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 Mode** Interface configuration mode/Global configuration mode

**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.

**Configuration Examples** The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from SVI1 to 120 seconds.

```
Ruijie(config)# interface vlan1
Ruijie(config-if-VLAN 1)# arp timeout 120
```

**Related Commands**

| Command                | Description                         |
|------------------------|-------------------------------------|
| <b>clear arp-cache</b> | Clears the ARP cache list.          |
| <b>show interface</b>  | Displays the interface information. |

**Platform** N/A

**Description**

## 2.8 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          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

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

**Command Mode** Interface configuration mode

**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**

```
Ruijie(config)# interface vlan1
Ruijie(config-if- VLAN 1)# arp trust-monitor enable
The following example disables engress gateway trusted ARP.
Ruijie(config)# interface vlan1
Ruijie(config-if- VLAN 1)# no arp trust-monitor enable
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 2.9 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** [ *trusted* ] [ *ip* [ *mask* ] ] | **interface** *interface-name* ]

**Parameter Description**

| Parameter                              | Description                                                                                                                                                                                                                                              |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>trusted</b>                         | Deletes trusted ARP cache. The dynamic ARP cache will be 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.                                                                                                                                    |

**Command Mode** Privileged EXEC mode

**Usage Guide** This command can be used to refresh an ARP cache table.

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** The following example deletes all dynamic ARP mapping records.

**Examples**

```
Ruijie# clear arp-cache
The following deletes the dynamic ARP entry 1.1.1.1.
Ruijie# clear arp-cache 1.1.1.1
```

The following example deletes the dynamic ARP entry on interface SV11.

```
Ruijie# clear arp-cache interface Vlan 1
```

**Related  
Commands**

| Command    | Description                                          |
|------------|------------------------------------------------------|
| <b>arp</b> | Adds a static mapping record to the ARP cache table. |

**Platform** N/A

**Description**

## 2.10 show arp

Use this command to display the Address Resolution Protocol (ARP) cache table

**show arp** [ *interface-type interface-number* | **trusted** [*ip [mask]*] | [*ip [mask]* | *mac-address* | **static** | **complete** | **incomplete** ] ]

**Parameter  
Description**

| Parameter               | Description                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>interface-type</i>   | Displays the ARP entry of a specified Layer-2 or Layer-3 port.                                                                                                                                     |
| <i>interface-number</i> |                                                                                                                                                                                                    |
| <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

**Usage Guide** N/A

**Configuration Examples** The following example displays the output result of the **show arp** command:

```
Ruijie# show arp
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
```

| 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 | Interface associated with the IP addresses                                                                                              |

The following example displays the output result of `show arp 192.168.195.68`

```
Ruijie# 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`

```
Ruijie# 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`

```
Ruijie# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A

## 2.11 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

**show arp counter**

**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 output result of the **show arp counter** command:

**Examples**

```
Ruijie#sho arp counter
ARP Limit: 256
Count of static entries: 0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total: 1
```

The following example displays the output result of the **show arp counter** command. The values following “overlayer” and “underlayer” indicate the number of ARP entries in the VxLAN and non-VxLAN respectively:

```
Ruijie#sho arp counter
ARP Limit: 256
Count of static entries: 0
Count of dynamic entries: 1 (complete: 1 incomplete: 0)
Total: 1 (overlayer: 0 underlayer: 1)
```

**Related**

**Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 2.12 show arp detail

Use this command to display the details of the Address Resolution Protocol (ARP) cache table.

**show arp detail** [ *interface-type interface-number* ] [ *ip [mask]* ] *mac-address* | **static** | **complete** | **incomplete** ]

**Parameter Description**

| Parameter                              | Description                                                               |
|----------------------------------------|---------------------------------------------------------------------------|
| <i>interface-type interface-number</i> | Displays the ARP of the layer 2 port or the layer 3 interface.            |
| <i>ip</i>                              | Displays the ARP entry of the specified IP address.                       |
| <i>ip mask</i>                         | Displays the ARP entries of the network segment included within the mask. |
| <i>mac-address</i>                     | Displays the ARP entry of the specified MAC address.                      |
| <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.                          |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port.  
 If you enter a *min\_value* greater than *max\_value*, no error message is prompted. Instead, ARP entries corresponding to the subvlan are displayed.

**Configuration** The following example displays the output result of the **show arp detail** command:

```
Examples IP Address MAC Address Type Age(min) Interface Port
192.168.183.65 0074.9c14.6e96 Dynamic 29 V11 Gi0/1
192.168.183.70 0074.9c4b.0c0f Local -- V11 --
Total number of ARP entries: 2
```

| Field       | Description                                          |
|-------------|------------------------------------------------------|
| IP Address  | IP address corresponding to the hardware address     |
| MAC Address | hardware address corresponding to the IP address     |
| Type        | ARP type, includes the Static, Dynamic, Trust, Local |
| Age         | Age of the ARP learning, in minutes                  |
| Interface   | Layer 3 interface associated with the IP addresses   |
| Port        | Layer2 port associated with the ARP                  |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 2.13 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.

**Usage Guide** N/A

**Configuration** The following example displays the output information of the command.

**Examples**

```
Ruijie# 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
```

| 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**

## 2.14 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the interface.

**show arp timeout**

| 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 the output of the **show arp timeout** command:

**Examples**

```
Ruijie# show arp timeout
Interface arp timeout(sec)

VLAN 1 3600
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 2.15 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

**show ip arp**

| 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 the output of **show ip arp**:

**Examples**

```
Ruijie# 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
```

| 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.                                                                                               |

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A



## 3 DHCP Commands

### 3.1 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 ID address by the DHCP by default.

**Command Mode** Interface configuration 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. At present, our server can support this function.

**Configuration** The following example makes the SVI1 port obtain the IP address automatically.

**Examples**

```
Ruijie(config)# interface vlan1
Ruijie(config-if- VLAN 1) ip address dhcp
```

| Related Commands | Command             | Description                                                                                    |
|------------------|---------------------|------------------------------------------------------------------------------------------------|
|                  | <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**

### 3.2 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 |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC 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**

```
Ruijie# show dhcp lease
Temp IP addr: 0.0.0.0 for peer on Interface: VLAN 1
Temp sub net mask: 0.0.0.0
 DHCP Lease server: 0.0.0.0, state: 3 Init-proc
 Retry count: 14993 Client-ID: 0100d0f8223363564C414E31
Temp IP addr: 172.18.23.245 for peer on Interface: VLAN 4094
Temp sub net mask: 255.255.255.0
 DHCP Lease server: 172.18.18.1, state: 7 Bound
 DHCP transaction id: c93c7c80
 Lease: 3600 secs, Renewal: 1800 secs, Rebind: 3150 secs
 Next timer fires after: 1648 secs
 Retry count: 14528 Client-ID: 0100d0f8223363564C414E34303934
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 4 DNS Commands

### 4.1 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.

```
Ruijie(config)#clear host *
```

| Related Commands | Command           | Description                          |
|------------------|-------------------|--------------------------------------|
|                  | <b>show hosts</b> | Displays the host name buffer table. |

**Platform** N/A

**Description**

### 4.2 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**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

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

**Command Mode** Global configuration mode.

**Usage Guide** This command enables the domain name resolution function.

**Configuration** The following example disables the DNS domain name resolution function.

**Examples** Ruijie(config)# no ip domain-lookup

**Related  
Commands**

| Command           | Description                                         |
|-------------------|-----------------------------------------------------|
| <b>show hosts</b> | Displays the DNS related configuration information. |

**Platform** N/A

**Description**

## 4.3 ip host

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 ip-address*

**no ip host** *host-name 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** SVI port or Layer 3 port.

**Usage Guide** N/A

**Configuration** The following example adds 192.168.21.139 as the auto-checking PD device.

**Examples** Ruijie(config-if-VLAN 1)#poE auto-checking pd-address 192.168.21.139 interface gigabitEthernet 0/1

**Related  
Commands**

| Command                       | Description                                           |
|-------------------------------|-------------------------------------------------------|
| <b>show poe auto-checking</b> | Show the PoE auto-checking configuration information. |

**Platform** N/A

**Description**

## 4.4 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* }

**no ip name-server** [ *ip-address* ]

**Parameter Description**

| Parameter         | Description                               |
|-------------------|-------------------------------------------|
| <i>ip-address</i> | The IP address of the domain name server. |

**Defaults** No domain name server is configured by default.

**Command Mode** Global configuration 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 sets the IP address of the domain name server to 192.168.5.134.

**Examples** Ruijie(config)# ip name-server 192.168.5.134

**Related Commands**

| Command           | Description                                         |
|-------------------|-----------------------------------------------------|
| <b>show hosts</b> | Displays the DNS related configuration information. |

**Platform** N/A

**Description**

## 4.5 show hosts

Use this command to display DNS configuration.

**show hosts** [ *hostname* ]

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                       |                                                 |
|-----------------------|-------------------------------------------------|
| <code>hostname</code> | Displays the specified domain name information, |
|-----------------------|-------------------------------------------------|

**Defaults** All domain name information is displayed by default.

**Command Mode** Privileged EXEC mode.

**Usage Guide** This command is used to display the DNS related configuration information.

```

Configuration Ruijie# show hosts
Examples Name servers are:
192.168.5.134 static
192.168.58.110 dynamic from DHCP
192.168.58.111 dynamic from DHCP
Host type Address TTL(sec)
switch static 192.168.5.243 ---
www.ruijie.com dynamic 192.168.5.123 126

```

| Field        | Description                                                   |
|--------------|---------------------------------------------------------------|
| Name servers | Domain name server                                            |
| Host         | Domain name                                                   |
| type         | Resolution type:<br>Static resolution and dynamic resolution. |
| Address      | IP address corresponding to the domain name                   |
| TTL          | TTL of entries corresponding to the domain name/IP address.   |

| Related Commands | 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** N/A

**Description**

## 5 Network Connectivity Test Tool Commands

### 5.1 ping

Use this command to test the connectivity of a network to locate the network connectivity problem. The command format is as follows:

```
ping [ip] [address [length length] [ntimes times] [timeout seconds] [data data] [source source] [df-bit] [validate] [detail] [out-interface interface]]
```

| Parameter | Parameter        | Description                                                                                                                                                 |
|-----------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <i>address</i>   | Specifies an IPv4 address.                                                                                                                                  |
|           | <i>length</i>    | Specifies the length of the packet to be sent (range: 36-18024, default: 100).                                                                              |
|           | <i>times</i>     | Specifies the number of packets to be sent (range:1-4294967295).                                                                                            |
|           | <i>seconds</i>   | Specifies the timeout time (range: 1-10 seconds).                                                                                                           |
|           | <i>data</i>      | Specifies the data to fill in.                                                                                                                              |
|           | <i>source</i>    | Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address. |
|           | <b>df-bit</b>    | Sets the DF bit for the IP address. DF bit=1 indicates not to segment the datagrams. By default, the DF bit is 0.                                           |
|           | <b>validate</b>  | Sets whether to validate the reply packets or not.                                                                                                          |
|           | <b>detail</b>    | Sets whether to contain details in the echoed message. By default, only “!” and “.” are displayed.                                                          |
|           | <i>interface</i> | Specifies the outbound interface                                                                                                                            |

**Defaults** Five packets with 100Byte in length are sent to the specified IP address within specified time (2s by default).

**Command** Privileged EXEC mode.

**Mode**

**Usage** If the device can be pinged, the response information is displayed, and the statistics is listed at the end. For the extension functions of ping, the number, quantity and timeout time of the packets to be sent can be specified, and the statistics is also displayed in the end. To use the domain name function, configure the domain name server firstly. For the concrete configuration, refer to the DNS Configuration section.

**Configuration** The following example tests the connectivity of a network to locate the network connectivity problem.

**ion**

**Examples**

 (The products do not support the VRF parameter. The following example is for reference purpose.)

Please take the actual device as the standard.)

The following example tests the connectivity of a network to locate the network connectivity problem (regular ping).

```
Ruijie# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
 < press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example displays details.

```
Ruijie#ping 192.168.21.26 detail
*Apr 16 09:16:08: %PING-7-DEBUG: Ping vrf index -1.
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
 < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.2
```

The following example tests the connectivity of a network to locate the network connectivity problem (extension ping).

```
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99
timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
 < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

The following example displays the details.

```
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3
detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
 < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
```



```

Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms

```

| Related Command | Command | Description |
|-----------------|---------|-------------|
| s               | N/A     | N/A         |

Platform N/A

Description

## 5.2 traceroute

Use this command to display all gateways passed by the test packets from the source address to the destination address.

**traceroute** [ *ip* ] [ *address* [ *probe number* ] [ *source source* ] [ *timeout seconds* ] [ *tll minimum maximum* ] [ *out-interface interface* ]]

| Parameter Description | Parameter              | Description                                                                                                                                                 |
|-----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>address</i>         | Specifies an IPv4 address.                                                                                                                                  |
|                       | <i>number</i>          | Specifies the number of probe packets to be sent (range: 1-255).                                                                                            |
|                       | <i>source</i>          | Specifies the source IPv4 address or the source interface. The loopback interface address (for example: 127.0.0.1) is not allowed to be the source address. |
|                       | <i>seconds</i>         | Specifies the timeout time (range: 1-10 seconds).                                                                                                           |
|                       | <i>minimum maximum</i> | Specifies the minimum and maximum TTL values (range:1-255).                                                                                                 |
|                       | <i>interface</i>       | Specifies the outbound interface                                                                                                                            |

**Defaults** By default, *seconds* is 3 seconds, *number* is 3, *minimum* and *maximum* are 1 and 255.

**Command Mode** Privileged EXEC mode: enables extended functions.  
 User EXEC mode: enables basic functions.

**Usage Guide** Use the **tracert** command to test the connectivity of a network to exactly locate the network connectivity problem when the network failure occurs. To use the function domain name, configure the domain name server. For the concrete configuration, refer to the DNS Configuration part.

**Configuration Examples** The following is two examples of the application about tracert, the one is of the smooth network, and the other is the network in which some gateways aren't connected successfully.

1. When the network is connected smoothly:

```
Ruijie# tracert 61.154.22.36
 < press Ctrl+C to break >
Tracing the route to 61.154.22.36

 1 192.168.12.1 0 msec 0 msec 0 msec
 2 192.168.9.2 4 msec 4 msec 4 msec
 3 192.168.9.1 8 msec 8 msec 4 msec
 4 192.168.0.10 4 msec 28 msec 12 msec
 5 192.168.9.2 4 msec 4 msec 4 msec
 6 202.101.143.154 12 msec 8 msec 24 msec
 7 61.154.22.36 12 msec 8 msec 22 msec
```

From above result, it's clear to know that the gateways passed by the packets sent to the host with an IP address of 61.154.22.36 (gateways 1~6) and the spent time are displayed. Such information is helpful for network analysis.

2. When some gateways in the network fail:

```
Ruijie# tracert 202.108.37.42
 < press Ctrl+C to break >
Tracing the route to 202.108.37.42

 1 192.168.12.1 0 msec 0 msec 0 msec
 2 192.168.9.2 0 msec 4 msec 4 msec
 3 192.168.110.1 16 msec 12 msec 16 msec
 4 * * *
 5 61.154.8.129 12 msec 28 msec 12 msec
 6 61.154.8.17 8 msec 12 msec 16 msec
 7 61.154.8.250 12 msec 12 msec 12 msec
 8 218.85.157.222 12 msec 12 msec 12 msec
 9 218.85.157.130 16 msec 16 msec 16 msec
10 218.85.157.77 16 msec 48 msec 16 msec
11 202.97.40.65 76 msec 24 msec 24 msec
12 202.97.37.65 32 msec 24 msec 24 msec
13 202.97.38.162 52 msec 52 msec 224 msec
14 202.96.12.38 84 msec 52 msec 52 msec
15 202.106.192.226 88 msec 52 msec 52 msec
16 202.106.192.174 52 msec 52 msec 88 msec
17 210.74.176.158 100 msec 52 msec 84 msec
```

```
18 202.108.37.42 48 msec 48 msec 52 msec
```

The above result clearly shown that the gateways passed by the packets sent to the host with an IP address of 202.108.37.42 (gateways 1~17) and the spent time are displayed, and gateway 4 fails.

3. The following example enables bout traceroute by entering a domain name.

```
Ruijie# traceroute www.ietf.org

Translating "www.ietf.org"...[OK]
 < press Ctrl+C to break >
Tracing the route to 64.170.98.32

 1 192.168.217.1 0 msec 0 msec 0 msec
 2 10.10.25.1 0 msec 0 msec 0 msec
 3 10.10.24.1 0 msec 0 msec 0 msec
 4 10.10.30.1 10 msec 0 msec 0 msec
 5 218.5.3.254 0 msec 0 msec 0 msec
 6 61.154.8.49 10 msec 0 msec 0 msec
 7 202.109.204.210 0 msec 0 msec 0 msec
 8 202.97.41.69 20 msec 10 msec 20 msec
 9 202.97.34.65 40 msec 40 msec 50 msec
10 202.97.57.222 50 msec 40 msec 40 msec
11 219.141.130.122 40 msec 50 msec 40 msec
12 219.142.11.10 40 msec 50 msec 30 msec
13 211.157.37.14 50 msec 40 msec 50 msec
14 222.35.65.1 40 msec 50 msec 40 msec
15 222.35.65.18 40 msec 40 msec 40 msec
16 222.35.15.109 50 msec 50 msec 50 msec
17 * * *
18 64.170.98.32 40 msec 40 msec 40 msec
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description**

N/A

## 6 TCP Commands

### 6.1 ip tcp keepalive

Use this command to enable the TCP keepalive function. Use the **no** form of this command to restore the default setting.

**ip tcp keepalive** [ **interval** *num1* ] [ **times** *num2* ] [ **idle-period** *num3* ]

**no ip tcp keepalive**

#### 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 Mode** Global configuration 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.

```
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

#### Related Commands

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** Introduced in the 11.0 version, this command replaces the **service tcp-keepalives-in** and **service tcp-keepalives-out** commands in 10.x versions.

## 6.2 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** The default MSS = Outgoing IPv4/v6 MTU- IPv4/v6 header-TCP header.

**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** The following example sets the upper limit of the MSS value to 1300 bytes.

**Examples** Ruijie(config)# ip tcp mss 1300

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 6.3 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** Ruijie(config)# ip tcp path-mtu-discovery

**Related  
Commands**

| Command       | Description                                  |
|---------------|----------------------------------------------|
| show tcp pmtu | Shows the PMTU value for the TCP connection. |

**Platform** N/A

**Description**

## 6.4 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.

```
Ruijie(config)# no ip tcp send-reset
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** The **ip tcp not-send-rst** command in version 10.x is disused but compatible in version 11.0. If this command is executed, it will be converted to the **no ip tcp send-reset** command.

## 6.5 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.

```
Ruijie(config)# ip tcp synwait-time 10
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** When run on the 11.0 version, the **ip tcp syntime-out** 10.x version command, which is no longer valid on the 11.0 version, is automatically transferred to the **ip tcp synwait-time** command.

**Description**

## 6.6 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> | Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes. |

**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.

The sending buffer is used to buffer the data of application programs. Each byte in the sending buffer has a sequence number, and bytes with sequence numbers acknowledged will be removed from the sending buffer. Increasing the sending buffer will improve the interaction between TCP and application programs, thus enhancing the performance. However, increasing the receiving buffer and sending buffer will result in more memory consumption of TCP.

This command is used to change the size of receiving buffer and sending buffer for TCP connections. This command changes both the receiving buffer and sending buffer, and only applies to subsequent connections. This command applies to both IPv4 and IPv6 TCP.

**Configuration** The following example sets the TCP window size to 16386 bytes.

**Examples**

```
Ruijie(config)# ip tcp window-size 16386
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**



## 6.7 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**

```
Ruijie#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
```

The following example displays the current IPv4 TCP connection statistics.

```
Ruijie#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
```

| 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 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**

## 6.8 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**

```
Ruijie#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
```

| Field                         | Description                                           |
|-------------------------------|-------------------------------------------------------|
| Hash table information        | Hash table information of the TCP session.            |
| Memory information            | Memory information of the TCP session.                |
| SYN specific information      | SYN information of the TCP session.                   |
| Timewait specific information | Information about the TCP session in timewait status. |
| Keepalive information         | TCP keepalive information.                            |
| MTU probing                   | MTU probing information.                              |
| FIN specific information      | Information about closing the TCP session.            |
| Orphan socket information     | Orphan socket information of the TCP session.         |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 6.9 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**

```
Ruijie# 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** N/A

**Description**

## 6.10 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**

```
Ruijie#sh tcp port
tcp port status:
Tcpv4 listen on 2650 have connections:
TCB Foreign Address Port State
Tcpv4 listen on 2650 have total 0 connections.
Tcpv4 listen on 23 have connections:
TCB Foreign Address Port State
c340800 1.1.1.2 64571 ESTABLISHED
Tcpv4 listen on 23 have total 1 connections.
Tcpv6 listen on 23 have connections:
```

| TCB     | Foreign Address | Port  | State       |
|---------|-----------------|-------|-------------|
| c429980 | 3000::2         | 64572 | ESTABLISHED |

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCB             | The control block's location in the current memory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Foreign Address | Remote address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Port            | Remote port number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| State           | <p>Status of the current 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.</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> |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

### 6.11 show tcp statistics

Use this command to show TCP statistics on received packets, three way handshake and time-wait.  
**show tcp statistics**

| 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 shows TCP parameters.

```

Examples Ruijie#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                                                                                                                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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                                                                                                                                                                                                                                                                                                                      |

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

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

## 7 IPv4 REF Commands

### 7.1 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-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 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**

```
Ruijie#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 forward1 0 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
```

| Field | Description      |
|-------|------------------|
| id    | Adjacent node ID |



|           |                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| state     | Adjacent node state:<br>Unresolved<br>Resolved                                                                                                                   |
| type      | Adjacent node type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>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                                               |
|------------------|--------------------------|-----------------------------------------------------------|
|                  | <b>show ip ref route</b> | Displays all route information in the current REF module. |

**Platform** N/A

**Description**

## 7.2 show ip ref exact-route

This command is used to display the IPv4 REF exact route.

**show ip ref exact-route** *source\_ipaddress dest\_ipaddress*

| Parameter          | Parameter               | Description                          |
|--------------------|-------------------------|--------------------------------------|
| <b>Description</b> | <i>source_ipaddress</i> | Source IP address of the packet      |
|                    | <i>dest_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** The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.

**Examples**

```
Ruijie# 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
```

| Field     | Description                                                                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id        | Adjacency ID                                                                                                                                                 |
| state     | Adjacency state:<br>Unresolved<br>Resolved                                                                                                                   |
| type      | Adjacency type<br>Local: local adjacency<br>Forward: forward adjacency<br>Discard: discard adjacency<br>Glean: glean adjacency<br>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 Commands | Command                  | Description                                                 |
|------------------|--------------------------|-------------------------------------------------------------|
|                  | <b>show ip ref route</b> | Displays all routing information in the current REF module. |

Platform N/A

Description

### 7.3 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** The following example displays IPv4 REF packet statistics.

**Examples** Ruijie #show ip ref packet 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**

## 7.4 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**

```
Ruijie#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<br>res: resolved                   |
| flags     | 0: related to adjacency<br>1: unrelated to adjacency |
| interface | Interface                                            |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 7.5 show ip ref route

Use this command to display all the routing information in the IPv4 REF table.

**show ip ref route [ default | ip mask | statistics ]**

**Parameter Description**

| Parameter         | Description                                       |
|-------------------|---------------------------------------------------|
| <b>default</b>    | Specifies the default route.                      |
| <i>ip</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** The following example displays all the routing information in the IPv4 REF table.

```

Examples Ruijie#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 GigabitEthernet 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 GigabitEthernet 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 GigabitEthernet 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                                                |
|------------------|--------------------------------|------------------------------------------------------------|
|                  | <b>show ip ref exact-route</b> | Displays the accurate REF forwarding path of an IP packet. |

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

# IP Routing Configuration Commands

---

## 1. NSM Commands

# 1 NSM 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.

```
clear ip route 192.168.12.0
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

### Platform

**Description** This command is not supported on 2-layer devices.

## 1.2 ip default-gateway

Use this command to configure the default gateway IP address on 2-layer devices. Use the **no** or **default** form of this command to restore the default setting.

**ip default-gateway** *ip-address*

**no ip default-gateway**

**default ip default-gateway**

| Parameter          | Parameter         | Description                         |
|--------------------|-------------------|-------------------------------------|
| <b>Description</b> | <i>ip-address</i> | IPv4 address of the default gateway |

**Defaults** No gateway IP address is configured by default.

### Command

**Mode** Global configuration mode

**Usage** When the device does not know the destination address of a packet, the device will forward the packet to the default gateway.

**Guide**

**Examples** The following example sets the IP address of default gateway to 192.168.1.1.

```
ip default-gateway 192.168.1.1
```

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

### Platform

**Description** This command is supported on 2-layer 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**

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

### Command

**Mode** Global configuration mode

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.

### Usage Guide

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.

```
Ruijie(config)# no ip routing
```

**Related Commands** N/A

**Platform**

**Description** This command is not supported on 2-layer devices.

## 1.4 show ip route

Use the commands to display the configuration of the IP routing table.

```
show ip route [[network [mask [longer-prefix]] | count | protocol [process-id]]]
```

```
show ip route [[normal | ecmp] [network [mask]]]
```

| 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-prefix</b> | (optional) Displays the routes that match the specified prefix.                                  |
| <b>count</b>         | (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.                                  |
| <i>process-id</i>    | (Optional) Routing protocol process ID.                                                          |
| <b>normal</b>        | Displays normal routes and not equivalent routes or fast reroutes.                               |
| <b>ecmp</b>          | Displays only equivalent routes.                                                                 |

**Defaults** All routes are displayed by default.

**Command Mode** Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

This command can display route information flexibly.

**Usage Guide** This command shows all routes. To show different attributes of routes, specify normal | ecmp | fast-reroute.

The following example displays the configuration of the IP routing table.

```
Ruijie# 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, EV - BGP EVPN, A - Arp to host
 LA - Local aggregate route
```

```

* - candidate default
Gateway of last resort is no set
S* 0.0.0.0/0 [1/0] via 172.18.23.1
C 172.18.23.0/24 is directly connected, VLAN 4094
C 172.18.23.204/32 is local host.

```

| Field          | Description                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S              | Source routing protocol, which may be:<br>C: directly connected route<br>S: static route<br>R: RIP route<br>B: BGP route<br>O: OSPF route<br>I: IS-IS route |
| 172.18.23.0/24 | Network address and mask of the destination network                                                                                                         |
| [1/0]          | Administrative distance/metric                                                                                                                              |

```

Ruijie# show ip route 172.18.23.0

Routing entry for 172.18.23.0/24
 Distance 0, metric 0
 Routing Descriptor Blocks:
 directly connected, via VLAN 4094, 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 |

```

Ruijie# show ip route count
----- route info -----
the num of active route: 5

```

```

Ruijie#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
C 192.1.1.0/24 is directly connected, VLAN 1
C 192.1.1.254/32 is local host

```

```

Ruijie#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

```

### 1.5 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     | -                    | -           |
| Defaults        | N/A                  |             |
| Command         |                      |             |
| Mode            | Privileged EXEC mode |             |
| Usage guideline | N/A                  |             |

The following example displays the statistics of the global routing table.

```
Ruijie# show ip route summary
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

Memory: 192 bytes
Entries: 3, 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     |

The following example displays the statistics of all routing tables.

```
Ruijie# show ip route summary all
Codes: NORMAL - Normal route ECMP - ECMP route FRR - Fast-Reroute route

IP routing table count: 0
Total
Memory: 192 bytes
Entries: 3, 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     |

```
Global
Memory: 192 bytes
Entries: 3, 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**

| Field                                | Description                                                                                                                                       |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| NORMAL                               | Type of the table entries. Value:<br>NORMAL: common routes (not ECMP or FRR);<br>ECMP: equivalent route;<br>FRR: fast reroute;<br>TOTAL: total    |
| Memory                               | Memory occupied by the table.                                                                                                                     |
| Entries: x , based on route prefixes | Number of entries based on prefix                                                                                                                 |
| Entries: x , based on route nexthops | Number of entries based on next-hop                                                                                                               |
| Connected                            | Protocol type. Value:<br>Connected: direct connection;<br>Static: static;<br>RIP: RIP;<br>OSPF: OSPF;<br>ISIS: ISIS;<br>BGP: BGP;<br>TOTAL: total |
| IP routing table count               | Number of routing tables                                                                                                                          |
| Global                               | Name of routing table. Value:<br>Global: default routing table<br>Total: all routing tables                                                       |

# Multicast Configuration 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**

| Parameter<br>Description | Parameter                                                                                                                                                                                                                                                                                                                                   | Description |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                          | N/A                                                                                                                                                                                                                                                                                                                                         | N/A         |
| Defaults                 | N/A                                                                                                                                                                                                                                                                                                                                         |             |
| Command<br>Mode          | Privileged EXEC 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 <b>clear ip igmp snooping gda-table</b> command. |             |
| Configuration            | The following example clears the Group Destination Address (GDA) table.                                                                                                                                                                                                                                                                     |             |
| Examples                 | <pre>Ruijie# clear ip igmp snooping gda-table</pre>                                                                                                                                                                                                                                                                                         |             |
| Platform<br>Description  | N/A                                                                                                                                                                                                                                                                                                                                         |             |

## 1.2 clear ip igmp snooping statistics

Use this command to clear IGMP Snooping statistics.

**clear ip igmp snooping statistics**

| Parameter<br>Description | Parameter            | Description |
|--------------------------|----------------------|-------------|
|                          | N/A                  | N/A         |
| Defaults                 | N/A                  |             |
| Command<br>Mode          | Privileged EXEC mode |             |

**Usage Guide** This command is used to clear the IGMP Snooping statistics, which can be displayed by using the **show ip igmp snooping statistics** command.

**Configuration** The following example clears the IGMP Snooping statistics.

**Examples**

```
Ruijie# clear ip igmp snooping statistics
```

**Platform** N/A

**Description**

## 1.3 deny

Use this command to deny the forwarding of the multicast streams in the range specified by the profile.  
**deny**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** The forwarding of the multicast streams in the range specified by the profile is denied.

**Command Mode** Profile configuration mode

**Usage Guide** First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.

**Configuration** The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244.

**Examples**

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# deny
```

**Platform** N/A

**Description**

## 1.4 ip igmp profile

Use this command to create a profile and enter the IGMP profile configuration mode.

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

**ip igmp profile** *profile-number*

**no ip igmp profile** *profile-number*

**default ip igmp profile** *profile-number*

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|



|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| <b>Description</b>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                             |
|                      | <i>profile-number</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Configures the profile number in the range from 1 to 1,024. |
| <b>Defaults</b>      | No profile is created by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                             |
| <b>Command Mode</b>  | Global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                             |
| <b>Usage Guide</b>   | <p>The profile is a filter to permit/deny specified groups in the following steps:</p> <ul style="list-style-type: none"> <li>● Use the <b>ip igmp profile</b> command to create a profile and enter profile configuration mode.</li> <li>● Use the <b>range</b> command to define a profile range.</li> <li>● Use the <b>permit</b> command to permit this profile in the filtering, or use the <b>deny</b> command to deny this profile in the filtering.</li> <li>● If the <b>deny</b> command is used without any profile specified, all profiles in the profile are denied.</li> <li>● If the <b>permit</b> command is used without any profile specified, all profiles in the profile are permitted.</li> </ul> |                                                             |
| <b>Configuration</b> | The following example creates and permits profile 1 with addresses from 224.2.2.2 to 224.2.2.244.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                             |
| <b>Examples</b>      | <pre>Ruijie(config)# ip igmp profile 1 Ruijie(config-profile)# range 224.2.2.2 224.2.2.244 Ruijie(config-profile)# permit</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                             |
| <b>Platform</b>      | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                             |
| <b>Description</b>   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                             |

## 1.5 ip igmp snooping

Use this command to enable IGMP snooping and enter the IVGL mode.

**ip igmp snooping ivgl**

Use this command to enable IGMP snooping and enter the SVGL mode.

**ip igmp snooping svgl**

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.

**Command Mode** Global configuration mode

- Usage Guide**
- **IVGL (Independent VLAN Group Learning):** 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.
  - **SVGL (Shared VLAN Group Learning):** In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicast flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped.

 SVGL mode conflicts with the IP multicast function.

 PIM Snooping must depend on IVGL mode of IGMP Snooping. Use **no ip igmp snooping** command to disable IGMP Snooping after PIM Snooping is disabled.

**Configuration** The following example enables IGMP Snooping and enters the IVGL mode.

**Examples**

```
Ruijie(config)# ip igmp snooping ivgl
```

The following example enables IGMP Snooping and enters the SVGL mode.

```
Ruijie(config)# ip igmp snooping svgl
Ruijie(config)# ip igmp snooping svgl profile 1
```

**Platform** N/A

**Description**

## 1.6 ip igmp snooping dyn-mr-aging-time

Use this command to set the aging time of a dynamic routing interface.

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

**ip igmp snooping dyn-mr-aging-time** *seconds*

**no ip igmp snooping dyn-mr-aging-time**

**default ip igmp snooping dyn-mr-aging-time**

| Parameter Description | Parameter      | Description                                                         |
|-----------------------|----------------|---------------------------------------------------------------------|
|                       | <i>seconds</i> | Configures the aging time in seconds. The range is from 1 to 3,600. |

**Defaults** The default is 300 seconds.

**Command Mode** Global configuration mode

**Usage Guide** If a dynamic routing interface does not receive IGMP query packets or PIM hello packets before aged, this interface will be deleted.

When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.

**Configuration Examples** The following example sets the aging time of the routing interface that the switch learns dynamically to 100 seconds.

```
Ruijie(config)# ip igmp snooping dyn-mr-aging-time 100
```

**Platform** N/A

**Description**

## 1.7 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 Examples** The following example enables the fast leave function.

```
Ruijie(config)# ip igmp snooping fast-leave enable
```

**Platform** N/A

**Description**

## 1.8 ip igmp snooping filter

Use this command to specify the profile for ports.

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

**ip igmp snooping filter** *profile-number*  
**no ip igmp snooping filter** *profile-number*  
**default ip igmp snooping filter**

Use this command to specify the profile for VLANs.

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

**ip igmp snooping vlan** *vlan-id filter* *profile-number*  
**no ip igmp snooping vlan** *vlan-id filter*  
**default ip igmp snooping vlan** *vlan-id filter*

**Parameter Description**

| Parameter             | Description                                                 |
|-----------------------|-------------------------------------------------------------|
| <i>profile-number</i> | Configures the profile number in the range from 1 to 1,024. |

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

**Command Mode** Global configuration mode/Interface configuration mode

**Usage Guide** A specific profile must be created before association.  
 Configure the **ip igmp snooping filter** *profile-number* command in the interface configuration mode.  
 Configure the **ip igmp snooping vlan** *vlan-id filter* *profile-number* in the global configuration mode.

**Configuration Examples** The following example specifies profile 1 for interface GigabitEthernet 0/1.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip igmp snooping filter 1
```

**Platform Description** N/A

## 1.9 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. |             |     |     |  |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------|-----|-----|--|
| <b>Defaults</b>               | The default is 260 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                    |             |     |     |  |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                    |             |     |     |  |
| <b>Usage Guide</b>            | <p>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.</p> <p>When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by <b>host-aging-time</b>. 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 <b>ip igmp snooping host-aging-time</b> command is executed, the aging time will be determined by <b>host-aging-time</b>. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.</p> |                                                                    |             |     |     |  |
| <b>Configuration Examples</b> | The following example sets the aging time to 30 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                    |             |     |     |  |
|                               | <pre>Ruijie(config)# ip igmp snooping host-aging-time 30</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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                    |             |     |     |  |

## 1.10 ip igmp snooping I2-entry-limit

Use this command to set the maximum number of multicast groups.

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

**ip igmp snooping I2-entry-limit** *number*

**no ip igmp snooping I2-entry-limit**

**default ip igmp snooping I2-entry-limit**

| <b>Parameter Description</b> | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>number</i></td> <td>Number of multicast groups. The value ranges from 0 to 256.</td> </tr> </tbody> </table>                                                      | Parameter | Description | <i>number</i> | Number of multicast groups. The value ranges from 0 to 256. |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|---------------|-------------------------------------------------------------|
| Parameter                    | Description                                                                                                                                                                                                                                                                  |           |             |               |                                                             |
| <i>number</i>                | Number of multicast groups. The value ranges from 0 to 256.                                                                                                                                                                                                                  |           |             |               |                                                             |
| <b>Defaults</b>              | The default is 256.                                                                                                                                                                                                                                                          |           |             |               |                                                             |
| <b>Command Mode</b>          | Global configuration mode                                                                                                                                                                                                                                                    |           |             |               |                                                             |
| <b>Usage Guide</b>           | The maximum number of multicast groups includes the multicast groups in all ports of all VLANs (including dynamic and static multicast groups). When the number of multicast groups reaches the limit, learning new group records and configuring new static multicast group |           |             |               |                                                             |

ports are not allowed.

**Configuration** The following example sets the maximum number of multicast groups to 256.

**Examples**

```
Ruijie(config)# ip igmp snooping l2-entry-limit 256
```

| Related Commands | Command                      | Description |
|------------------|------------------------------|-------------|
|                  | <b>show ip igmp snooping</b> |             |

**Platform Description** N/A

## 1.11 ip igmp snooping max-groups

Use this command to configure the maximum number of groups that can be added dynamically to this interface.

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

**ip igmp snooping max-groups** *number*

**no ip igmp snooping max-groups**

**default ip igmp snooping max-groups**

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

**Defaults** No maximum group number is configured by default.

**Command Mode** Interface configuration mode

**Usage Guide** If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.

**Configuration Examples** The following example configures the maximum number of multicast groups to 100 on GigabitEthernet interface 0/1:

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if)# ip igmp snooping max-group 100
```

**Platform Description** N/A

## 1.12 ip igmp snooping mrouter learn pim-dvmrp

Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface

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

**ip igmp snooping [ vlan vid ] mrouter learn pim-dvmrp**  
**no ip igmp snooping [ vlan vid ] mrouter learn pim-dvmrp**  
**default ip igmp snooping [ vlan vid ] mrouter learn pim-dvmrp**

**Parameter  
Description**

| Parameter       | Description                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------|
| <b>vlan vid</b> | Configures the VLAN ID in the range from 1 to 4,094. By default, the specified version is supported on all VLANs. |

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

**Command**

**Mode** Global configuration mode

**Usage Guide** Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled).  
 By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.

**Platform** N/A

**Description**

## 1.13 ip igmp snooping preview

Use this command to allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

Use **no** or **default** form of this command to disable multicast preview.

**ip igmp snooping preview profile-number**  
**no ip igmp snooping preview**  
**default ip igmp snooping preview**

**Parameter  
Description**

| Parameter             | Description                                                 |
|-----------------------|-------------------------------------------------------------|
| <i>profile-number</i> | Configures the profile number in the range from 1 to 1,024. |

|                               |                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>               | This function is disabled by default.                                                                                                                                                                                                                                                                                                                                         |
| <b>Command Mode</b>           | Global configuration mode                                                                                                                                                                                                                                                                                                                                                     |
| <b>Usage Guide</b>            | Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview. |
| <b>Configuration Examples</b> | The following example associates the profile 2 to the GigabitEthernet interface 0/1 and associates multicast preview with profile 1.                                                                                                                                                                                                                                          |
|                               | <pre>Ruijie(config)# ip igmp snooping preview 1 Ruijie(config-if)# int GigabitEthernet 0/1 Ruijie(config-if)# ip igmp snooping filter 2</pre>                                                                                                                                                                                                                                 |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                                                                                                                                                                           |

## 1.14 ip igmp snooping preview interval

Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams.

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

**ip igmp snooping preview interval** *seconds*

**no ip igmp snooping preview interval**

**default ip igmp snooping preview interval**

| Parameter Description | Parameter      | Description                                           |
|-----------------------|----------------|-------------------------------------------------------|
|                       | <i>seconds</i> | Preview interval from 1 to 300 in the unit of seconds |

|                               |                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------|
| <b>Defaults</b>               | The default is 60 seconds.                                                                                  |
| <b>Command Mode</b>           | Global configuration mode                                                                                   |
| <b>Usage Guide</b>            | N/A                                                                                                         |
| <b>Configuration Examples</b> | The following example sets the multicast preview interval as 100 seconds on the 1000M port of 0/1:          |
|                               | <pre>Ruijie(config)# ip igmp snooping preview 1 Ruijie(config)# ip igmp snooping preview interval 100</pre> |



**Platform** N/A

**Description**

## 1.15 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**

| Parameter Description | Parameter              | Description                                                                                                       |
|-----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <b>vlan <i>vid</i></b> | Configures the VLAN ID in the range from 1 to 4,094. By default, the specified version is supported on all VLANs. |

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

**Command Mode** Global configuration mode

**Usage Guide** After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function.

If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.

**Configuration** The following example enables the IGMP querier function in VLAN 2.

**Examples**

```
Ruijie(config)# ip igmp snooping querier
Ruijie(config)# ip igmp snooping vlan 2 querier
```

**Platform** N/A

**Description**

## 1.16 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 *a.b.c.d***

**no ip igmp snooping [ vlan *vid* ] querier address**

**default ip igmp snooping [ vlan *vid* ] querier address**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

|                        |                                                                                                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>vlan</b> <i>vid</i> | Configures the VLAN ID in the range from 1 to 4,094. By default, the specified version is supported on all VLANs. |
| <i>a.b.c.d</i>         | 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** Ruijie(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.

Ruijie(config)# ip igmp snooping vlan 3 querier address 1.1.1.1

**Platform** N/A

**Description**

## 1.17 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                                                                                                       |
|-----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <i>num</i>             | Maximum response time from 1 to 25 in the unit of seconds                                                         |
|                       | <b>vlan</b> <i>vid</i> | Configures the VLAN ID in the range from 1 to 4,094. By default, the specified version is supported on all VLANs. |

**Defaults** The default is 10 seconds.

**Command Mode** Global configuration mode

**Usage Guide** 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**

```
Ruijie(config)# ip igmp snooping querier max-response-time 15
```

The following example specifies the maximum response time of the IGMP querier in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier max-response-time 15
```

**Platform** N/A

**Description**

## 1.18 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 [ vlan vid ] querier query-interval seconds**

**no ip igmp snooping [ vlan vid ] querier query-interval**

**default ip igmp snooping [ vlan vid ] querier query-interval**

| Parameter Description | Parameter       | Description                                                                                                       |
|-----------------------|-----------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i>  | Query interval from 1 to 18,000 in the unit of seconds                                                            |
|                       | <b>vlan vid</b> | Configures the VLAN ID in the range from 1 to 4,094. 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**

```
Ruijie(config)# ip igmp snooping querier query-interval 100
```

The following example configures the query interval in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier query-interval 100
```

**Platform** N/A

**Description**

## 1.19 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
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> | Configures the VLAN ID in the range from 1 to 4,094. 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 Examples** The following example configures the non-querier expiration timer on the device.

```
Ruijie(config)# ip igmp snooping querier timer expiry 60
```

The following example configures the non-querier expiration timer in VLAN 3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

**Platform Description** N/A

## 1.20 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
```

| Parameter Description | Parameter      | Description                                                                                                                     |
|-----------------------|----------------|---------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>seconds</i> | Configures the aging time of the routing interface that the switch learns dynamically in seconds, 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>Ruijie(config)# ip igmp snooping query-max-response-time 100</pre>                                                                                                                                                                                                                                                                                                     |
| <b>Platform Description</b>   | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## 1.21 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**

| Parameter Description | Parameter              | Description                                                                                                       |
|-----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------|
|                       | <b>vlan <i>vid</i></b> | Configures the VLAN ID in the range from 1 to 4,094. By default, the specified version is supported on all VLANs. |

**Defaults** The default version is IGMPv2.

**Command Mode** Global configuration mode

**Usage Guide** If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.

IGMPv1 and IGMPv2 are supported.

**Configuration Examples** The following example configures IGMP querier version on the device.

```
Ruijie(config)# ip igmp snooping querier version 1
```

The following example configures IGMP querier version on VLAN3.

```
Ruijie(config)# ip igmp snooping vlan 3 querier version 1
```

**Platform** N/A

**Description**

## 1.22 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** The following example enables IGMP snooping suppression on the device.

**Examples**

```
Ruijie(config)# ip igmp snooping suppression enable
```

**Platform** N/A

**Description**

## 1.23 ip igmp snooping svgl profile

Use this command to specify the multicast group address range applied in the SVGL/IVGL-SVGL mode.

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

**ip igmp snooping svgl profile** *profile-number*

**no ip igmp snooping svgl profile**

**default ip igmp snooping svgl profile**

**Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

|                       |                                                             |
|-----------------------|-------------------------------------------------------------|
| <i>profile-number</i> | Configures the profile number in the range from 1 to 1,024. |
|-----------------------|-------------------------------------------------------------|

**Defaults** No profile is associated.

**Command Mode** Global configuration mode

**Usage Guide** When the IGMP Snooping works in the SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode.

**Configuration Examples** The following example specifies the profile 2 applied in SVGL mode.

```
Ruijie(config)# ip igmp snooping svgl profile 2
```

**Platform** N/A

**Description**

## 1.24 ip igmp snooping svgl subvlan

Use this command to specify the subvlan of multicast VLAN.

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

**ip igmp snooping svgl subvlan** [*vid-range*]

**no ip igmp snooping svgl subvlan** [*vid-range*]

**default ip igmp snooping svgl subvlan** [ *vid-range* ]

| Parameter Description | Parameter        | Description                                          |
|-----------------------|------------------|------------------------------------------------------|
|                       | <i>vid-range</i> | Configures the VLAN ID or ID range, e.g., 1 and 3-5. |

**Defaults** By default, all VLANs except shared VLANs serve as its sub VLANs.

**Command Mode** Global configuration mode

**Usage Guide** This command only takes effect in SVGL mode.

**Configuration Examples** The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.

```
Ruijie(config)# ip igmp snooping svgl vlan 3
Ruijie(config)# ip igmp snooping svgl subvlan 2,5-7
```

**Platform** N/A

**Description**

## 1.25 ip igmp snooping svgl vlan

Use this command to specify the shared VLAN in SVGL mode.

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

**ip igmp snooping svgl vlan** *vid*

**no ip igmp snooping svgl vlan**

**default ip igmp snooping svgl vlan**

| Parameter Description | Parameter  | Description                                         |
|-----------------------|------------|-----------------------------------------------------|
|                       | <i>vid</i> | Configures the VLAN ID in the range from 1 to 4,094 |

**Defaults** By default , the shared VLAN is VLAN 1.

**Command Mode** Global configuration mode

**Usage Guide** This command only works in the SVGL mode.

**Configuration Examples** The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.

```
Ruijie(config)# ip igmp snooping svgl vlan 3
Ruijie(config)# ip igmp snooping svgl subvlan 2,5-7
```

**Platform Description** N/A

## 1.26 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*

| Parameter Description | Parameter  | Description                                         |
|-----------------------|------------|-----------------------------------------------------|
|                       | <i>vid</i> | Configures the VLAN ID in the range from 1 to 4,094 |

**Defaults** If IGMP Snooping (IVGL mode) is enabled globally, all VLANs are enabled with IGMP Snooping (IVGL mode).  
If IGMP Snooping (IVGL mode) is not enabled globally, all VLANs are not enabled with IGMP Snooping



(IVGL mode).

**Command Mode**

Global configuration mode

**Usage Guide**

Use this command to enable or disable the IGMP snooping on the specified VLAN.

**Configuration**

The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2.

**Examples**

```
Ruijie(config)# ip igmp snooping ivgl
Ruijie(config)# no ip igmp snooping vlan 2
```

**Platform**

N/A

**Description**

## 1.27 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>                                       | Configures the VLAN ID in the range from 1 to 4,094. |
| <i>interface-type</i><br><i>interface-number</i> | Interface ID                                         |

**Defaults**

No static routing interface is configured by default.

**Command Mode**

Global configuration mode

**Usage Guide**

A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age.

When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded.

When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.

**Configuration**

The following example configures a static routing interface.

**Examples**

```
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/1
```

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

## 1.28 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>          | Configures the 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.

```
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface
GigabitEthernet 0/1
```

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

## 1.29 permit

Use this command to permit the multicast forwarding for specified ranges of a specified profile.

**permit**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|-----------------------|-----------|-------------|

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

**Defaults** The forwarding of the multicast streams in the range specified by the profile is denied.

**Command Mode** Profile configuration mode

**Usage Guide** A profile is used to filter a group of multicast packets, so as to assist other features.  
Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.
3. Use the **permit** command to permit the multicast forwarding for the profile.

**Configuration Examples** The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1.

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# permit
```

**Platform Description** N/A

## 1.30 range

Use this command to define a range for a specific profile.  
Use the **no** form of the command to remove the range from the profile.  
**range** *low-ip-address* [*high-ip-address*]  
**no range** *low-ip-address* [*high-ip-address*]

| Parameter Description | Parameter              | Description              |
|-----------------------|------------------------|--------------------------|
|                       | <i>low-ip-address</i>  | Start address of a range |
|                       | <i>high-ip-address</i> | End address of a range   |

**Defaults** No range is defined for a profile by default.

**Command Mode** Profile configuration mode

**Usage Guide** A profile is used to filter a group of multicast packets, so as to assist other features.  
Configuration steps:

1. Use the **ip igmp profile** command to create a profile and enter profile configuration mode.
2. Use the **range** command to define a range for the profile.

- Use the **permit** command to permit the multicast forwarding for the profile.

**Configuration** The following is an example of allowingpermits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244: of profile 1.

**Examples**

```
Ruijie(config)# ip igmp profile 1
Ruijie(config-profile)# range 224.2.2.2 224.2.2.244
Ruijie(config-profile)# permit
```

**Platform** N/A

**Description**

### 1.31 show ip igmp profile

Use this command to display the profile information.

**show ip igmp profile** [ *profile-number* ]

**Parameter Description**

| Parameter             | Description                                                 |
|-----------------------|-------------------------------------------------------------|
| <i>profile-number</i> | Configures the profile number in the range from 1 to 1,024. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** Use this command to display the profile information.

**Configuration** The following example displays the profile information.

**Examples**

```
Ruijie(config-if)# show ip igmp profile
Profile 1
Permit
range 224.0.1.0, 239.255.255.255
```

### 1.32 show ip igmp snooping

Use this command to display related information of IGMP Snooping.

**show ip igmp snooping** [**gda-table** | **interfaces** *interface-type interface-number* | **mrouter** | **statistics** [**vlan vid**] | **querier** [ **detail** | **vlan vid** ] ]

**Parameter Description**

| Parameter       | Description                                                           |
|-----------------|-----------------------------------------------------------------------|
| <b>vlan vid</b> | Configures the VLAN ID in the range from 1 to 4,094. By default, IGMP |

|                                                  |                                                  |
|--------------------------------------------------|--------------------------------------------------|
|                                                  | Snooping information of all VLANs are displayed. |
| <i>interface-type</i><br><i>interface-number</i> | Interface type and number                        |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** N/A

**Configuration** The following example displays global IGMP Snooping information.

**Examples**

```
Ruijie#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 256
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2
IGMP Snooping version: 2IGMP 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.

```
Ruijie#show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 256
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**

## Security Configuration Commands

---

1. AAA Commands
2. Storm Control Commands
3. Password-Policy Commands
4. Port Security Commands
5. SSH Commands
6. CPU Protection Commands
7. DHCP Snooping Commands
8. ACL Commands
9. QoS 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, the TACACS+ server group is supported.                                            |

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

**Command Mode** Global configuration mode

**Usage Guide** RGOS enables the accounting command function after enabling the login authentication. 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**

```
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
```

| Related Commands | Command                    | Description                                           |
|------------------|----------------------------|-------------------------------------------------------|
|                  | <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 and TACACS+ server group is supported.                           |

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

**Command** Global configuration mode

**Mode**

**Usage Guide** RGOS enables the exec accounting function after enabling the login authentication. 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**

```
Ruijie(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 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          | Parameter | Description |
|--------------------|-----------|-------------|
| <b>Description</b> | N/A       | N/A         |

**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 Examples** The following example enables the accounting update function.

```
Ruijie(config)# aaa new-model
Ruijie(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**

### 1.4 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 range from 1 to 525,600 in the unit of minutes. |

- Defaults** The default is 5 minutes.
- Command** Global configuration mode
- 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**

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

| 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**

## 1.5 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 Description | Parameter      | 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> , <b>group</b> and <b>enable</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 and TACACS+ 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** The following example defines an AAA Enable authentication method list. In the authentication

**Examples** 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.

```
Ruijie(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**

## 1.6 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> , <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 and TACACS+ server groups are supported.                             |

**Defaults**

N/A

**Command** 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.

```
Ruijie(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**

## 1.7 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> , <b>group</b> and <b>local</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. At present, the TACACS+ server group is supported.                                   |
| <b>local</b>     | Uses the local user name database for authorization.                                                                          |

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

**Command Mode** Global configuration mode

**Usage Guide** RGOS 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 TACACS+ server to authorize the level 15 command.

**Examples** Ruijie(config)# aaa authorization commands 15 default group tacacs+

| 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 Description** N/A

## 1.8 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 Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | 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**

```
Ruijie(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**

## 1.9 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 Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

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

**Command Mode** Global configuration mode

**Usage Guide** RGOS supports to 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** The following example enables the aaa authorization console function.

**Examples**

```
Ruijie(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**

## 1.10 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 and TACACS+ server group is supported.               |

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

**Command** Global configuration mode

**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**

```
Ruijie(config)# aaa authorization exec default group radius
```

| Related  | Command                   | Description                                             |
|----------|---------------------------|---------------------------------------------------------|
| Commands | <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**



## 1.11 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                                                                                                             |
|-------------|----------------|-------------------------------------------------------------------------------------------------------------------------|
| Description | <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 and TACACS+ 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**

```
Ruijie(config)# aaa authorization network default group radius
```

| Related  | Command                   | Description                       |
|----------|---------------------------|-----------------------------------|
| Commands | <b>aaa new-model</b>      | Enables the AAA security service. |
|          | <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**

## 1.12 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** The following example sets login attempt times to 6.

**Examples**

```
Ruijie #configure terminal
Ruijie(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**

## 1.13 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 Mode** Global configuration 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**

```
Ruijie#configure terminal
Ruijie(config)#aaa local authentication lockout-time 5
```

**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**

## 1.14 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****Description**

| Parameter | 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**

```
Ruijie(config)# no aaa log enable
```

**Related****Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 1.15 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**

|                               |                                                                                                                                       |                                                                                                                                  |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Parameter</b>              | <b>Parameter</b>                                                                                                                      | <b>Description</b>                                                                                                               |
| <b>Description</b>            | <i>num</i>                                                                                                                            | The number of syslog entries printed per second. The range is from 0 to 65,535.<br>0 indicates the printing rate is not limited. |
| <b>Defaults</b>               | The default is 5.                                                                                                                     |                                                                                                                                  |
| <b>Command Mode</b>           | Global configuration mode                                                                                                             |                                                                                                                                  |
| <b>Usage Guide</b>            | Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate. |                                                                                                                                  |
| <b>Configuration Examples</b> | The following example sets the rate of printing the syslog informing AAA authentication success to 10.                                |                                                                                                                                  |
|                               | <pre>Ruijie(config)# aaa log rate-limit 10</pre>                                                                                      |                                                                                                                                  |
| <b>Related Commands</b>       | <b>Command</b>                                                                                                                        | <b>Description</b>                                                                                                               |
|                               | N/A                                                                                                                                   | N/A                                                                                                                              |
| <b>Platform Description</b>   | N/A                                                                                                                                   |                                                                                                                                  |

## 1.16 aaa new-model

Use this command to enable the RGOS AAA security service.

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

**aaa new-model**

**no aaa new-model**

|                     |                                                                                                    |                    |
|---------------------|----------------------------------------------------------------------------------------------------|--------------------|
| <b>Parameter</b>    | <b>Parameter</b>                                                                                   | <b>Description</b> |
| <b>Description</b>  | N/A                                                                                                | N/A                |
| <b>Defaults</b>     | This function is disabled by default.                                                              |                    |
| <b>Command Mode</b> | Global configuration mode                                                                          |                    |
| <b>Usage Guide</b>  | 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**

```
Ruijie(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**

## 1.17 clear aaa local user lockout

Use this command to clear the lockout user list.

**clear aaa local user lockout { all | user-name word }**

| Parameter          | Parameter             | Description                          |
|--------------------|-----------------------|--------------------------------------|
| <b>Description</b> | <b>all</b>            | Indicates all locked users.          |
|                    | <b>user-name word</b> | Indicates the ID of the locked User. |

**Defaults** N/A

**Command** Privileged EXEC mode

**Mode**

**Usage Guide** Use this command to clear all the user lists or a specified user list.

**Configuration** The following example clears the lockout user list.

**Examples**

```
Ruijie(config)# clear aaa local user lockout all
```

| 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**

## 1.18 show aaa accounting update

Use this command to display the accounting update information.

**show aaa accounting update**

|                         |                                                                                                                          |                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <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/Global configuration mode/Interface configuration mode                                              |                                            |
| <b>Usage Guide</b>      | Use this command to display the accounting update interval and whether the accounting update is enabled.                 |                                            |
| <b>Configuration</b>    | The following example displays the accounting update information.                                                        |                                            |
| <b>Examples</b>         | <pre>Ruijie# show aaa accounting update Accounting Update:          Disabled Accounting Update Interval: 5 Minutes</pre> |                                            |
| <b>Related Commands</b> | <b>Command</b>                                                                                                           | <b>Description</b>                         |
|                         | <b>aaa new-model</b>                                                                                                     | Enables the AAA security service.          |
|                         | <b>aaa domain enable</b>                                                                                                 | Enables the domain-name-based AAA service. |
| <b>Platform</b>         | N/A                                                                                                                      |                                            |
| <b>Description</b>      |                                                                                                                          |                                            |

## 1.19 show aaa lockout

Use this command to display the lockout configuration.

**show aaa lockout**

|                      |                                                                                   |                    |
|----------------------|-----------------------------------------------------------------------------------|--------------------|
| <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/Global configuration mode/Interface configuration mode       |                    |
| <b>Usage Guide</b>   | Use this command to display the lockout configuration.                            |                    |
| <b>Configuration</b> | The following example displays the lockout configuration.                         |                    |
| <b>Examples</b>      | <pre>Ruijie# show aaa lockout Lock tries:      3 Lock timeout:   15 minutes</pre> |                    |

| Related  | Command | Description |
|----------|---------|-------------|
| Commands | N/A     | N/A         |

Platform N/A

Description

## 1.20 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 Privileged EXEC mode/Global configuration mode/Interface configuration mode

Mode

Usage Guide N/A

Configuration The following command displays all the server groups.

Examples

```
Ruijie# show aaa group
Type Reference Name

radius 1 radius
tacacs+ 1 tacacs+
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

## 1.21 show aaa method-list

Use this command to display all AAA method lists.

**show aaa method-list**

| 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 all AAA method lists.

**Configuration** The following example displays the AAA method list.

**Examples**

```
Ruijie# 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         | Command                   | Description                               |
|-----------------|---------------------------|-------------------------------------------|
| <b>Commands</b> | <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**

## 1.22 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          | Parameter                       | Description                                                                |
|--------------------|---------------------------------|----------------------------------------------------------------------------|
| <b>Description</b> | <b>all</b>                      | Displays all AAA user information.                                         |
|                    | <b>lockout</b>                  | Displays the locked AAA user information.                                  |
|                    | <b>by-id <i>session-id</i></b>  | Displays the information of the AAA user that with a specified session ID. |
|                    | <b>by-name <i>user-name</i></b> | 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.

```
Ruijie#show aaa user all

 Id ----- Name
2345687901 wwxy

Ruijie# show aaa user by-id 2345687901

 Id ----- Name
2345687901 wwxy

Ruijie# show aaa user by-name wwxy

 Id ----- Name
2345687901 wwxy

Ruijie# show aaa user lockout
Name Tries Lock Timeout (min)

Ruijie#
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

## 2 Storm Control Commands

### 2.1 show storm-control

Use this command to display storm suppression information.

**show storm-control** [ *interface-type interface-number* ]

| Parameter Description | Parameter                                        | Description             |
|-----------------------|--------------------------------------------------|-------------------------|
|                       | <i>interface-type</i><br><i>interface-number</i> | Specifies an interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode/Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example displays storm control configuration on GigabitEthernet 0/1.

```
Ruijie# show storm-control gigabitethernet 0/1
Interface Broadcast Control Multicast Control Unicast Control
Action

GigabitEthernet 0/1 1 % 50 % 1 %
none
```

| Related Commands | Command              | Description                |
|------------------|----------------------|----------------------------|
|                  | <b>storm-control</b> | Enables storm suppression. |

**Platform Description** N/A

### 2.2 storm-control

Use this command to enable the storm suppression for unknown unicast packets.

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

**storm-control unicast** [ *level percent* | **pps** *packets* | *rate-bps* ]

**no storm-control unicast**

**default storm-control unicast**

Use this command to enable the storm suppression for multicast packets.

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

**storm-control multicast** [ *level percent* | **pps packets** | *rate-bps* ]

**no storm-control multicast**

**default storm-control multicast**

Use this command to enable the storm suppression for broadcast packets.

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

**storm-control broadcast** [ *level percent* | **pps packets** | *rate-bps* ]

**no storm-control broadcast**

**default storm-control broadcast**

**Parameter  
Description**

| Parameter            | Description                                               |
|----------------------|-----------------------------------------------------------|
| <i>level percent</i> | Sets the bandwidth percentage, for example, 20 means 20%. |
| <b>pps packets</b>   | Sets the pps, which means packets per second.             |
| <i>rate-bps</i>      | Rate allowed in the unit of 64 to 1,000,000.              |

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

**Command  
Mode** Interface configuration mode

**Usage Guide** Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms.

A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).

**Configuration  
Examples** The following example enables the multicast storm suppression on GigabitEthernet 0/1 and sets the allowed rate to 4M.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# storm-control multicast 4096
```

**Related  
Commands**

| Command                   | Description                             |
|---------------------------|-----------------------------------------|
| <b>show storm-control</b> | Displays storm suppression information. |

**Platform  
Description** N/A

### 3 Password-Policy Commands

#### 3.1 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** The following example sets the password lifecycle to 90 days.

**Examples**

```
Ruijie(config)# password policy life-cycle 90
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform Description** N/A

#### 3.2 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<br>Description | Parameter | Description   |
|--------------------------|-----------|---------------|
|                          |           | <i>length</i> |

**Defaults** No minimum length of the password is set by default.

**Command Mode** Global configuration 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** Ruijie(config)# password policy min-size 8

| Related<br>Commands | Command | Description |
|---------------------|---------|-------------|
|                     |         | N/A         |

**Platform Description** N/A

### 3.3 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<br>Description | Parameter | Description  |
|--------------------------|-----------|--------------|
|                          |           | <i>times</i> |

**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**

```
Ruijie(config)# password policy no-repeat-times 5
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

## 3.4 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**

```
Ruijie(config)# password policy strong
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A

### 3.5 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**

```
Ruijie(config)# service password-encryption
```

**Related  
Commands**

| Command                | Description                             |
|------------------------|-----------------------------------------|
| <b>enable password</b> | Sets passwords of different privileges. |

**Platform  
Description**

N/A

### 3.6 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.

```
Ruijie#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



## 4 Port Security Commands

### 4.1 switchport port-security

Use this command to configure port security and the way to deal with violation.

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

**switchport port-security** [ violation { protect | restrict | shutdown } ]



**no switchport port-security** [ violation ]

| Parameter Description | Parameter        | Description                                                                                     |
|-----------------------|------------------|-------------------------------------------------------------------------------------------------|
|                       | <b>violation</b> | Configures the way to deal with violation.                                                      |
|                       | <b>protect</b>   | Discards the packets breaching security.                                                        |
|                       | <b>restrict</b>  | Discards the packets breaching security and sends the Trap message.                             |
|                       | <b>shutdown</b>  | Discards the packets breaching the security, sends the Trap message and disables the interface. |

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

**Command Mode** Interface configuration mode

**Usage Guide** With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.

-  If the violation handling mode is changed after violation occurs, the new mode takes effect only after the violation mode is restarted.
-  When the port security and 802.1x are configured at the same time, secure ports do not generate dynamic secure address entries.

**Configuration Examples** The following example enables port security on interface gigabitethernet 0/1, and the way to deal with violation is **shutdown**:

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security violation
shutdown
```

| Related Commands | Command | Description               |
|------------------|---------|---------------------------|
|                  |         | <b>show port-security</b> |

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

## 4.2 switchport port-security aging

Use this command to set the aging time for all secure addresses on an interface.

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

**switchport port-security aging { static | time *time* }**

**no switchport port-security aging { static | time }**

| Parameter Description | Parameter               | Description                                                                                                                                                 |
|-----------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                         | <b>static</b>                                                                                                                                               |
|                       | <b>time <i>time</i></b> | Specifies the aging time for the secure address on this port. Its range is 0-1,440 in minutes. If you set it to 0, the aging function is disabled actually. |


**Defaults** No secure address is aged by default.

**Command Mode** Interface configuration mode

**Usage Guide** In interface configuration mode, use the **no switchport port-security aging time command** to disable the aging for security addresses on the port. Use the **no switchport port-security aging static** command to apply the aging time to only the dynamically learned security address.

Use the **show port-security** command to display configuration.

When both port security and 802.1X authentication functions are enabled, 802.1X clients must get re-authenticated for network access once the secure addresses are aged.

 To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface.

**Configuration Examples** The following example sets the aging time for all secure addresses on interface gigabitethernet 0/1 to eight minutes.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# switchport port-security aging time 8
```

```
Ruijie(config-if-GigabitEthernet 0/1) # switchport port-security aging static
Ruijie(config-if) # end
```

**Related  
Commands**

| Command                   | Description                      |
|---------------------------|----------------------------------|
| <b>show port-security</b> | Displays port security settings. |

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

### 4.3 switchport port-security binding

Use these commands to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

**switchport port-security binding** [ *mac-address* **vlan** *vlan\_id* ] *ipv4-address*

**no switchport port-security binding** [ *mac-address* **vlan** *vlan\_id* ] *ipv4-address*

**Parameter  
Description**

| Parameter                  | Description                               |
|----------------------------|-------------------------------------------|
| <i>mac-address</i>         | The source MAC addresses to be bound      |
| <b>vlan</b> <i>vlan_id</i> | VLAN ID of the binding source MAC address |
| <i>ipv4-address</i>        | Binds IPv4 addresses.                     |

**Defaults** N/A

**Command  
Mode** Interface configuration mode

**Usage Guide**

1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

Network is often accessible to static users with secure addresses without authorization. If authorization is configured, these users must comply with it.

**Configuration** The following example binds the IP address 192.168.1.100 on interface g 0/10:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10) # switchport port-security binding
192.168.1.100
Ruijie(config-if-GigabitEthernet 0/10) # end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport port-security binding
00d0.f800.5555 vlan 1 192.168.1.100
Ruijie(config-if-GigabitEthernet 0/10)# end
```

#### Related Commands

| Command                                           | Description                                                    |
|---------------------------------------------------|----------------------------------------------------------------|
| <b>show port-security</b>                         | Displays port security settings.                               |
| <b>switchport port-security</b>                   | Enables the port-security.                                     |
| <b>switchport port-security binding interface</b> | Configures the secure address binding in privileged EXEC mode. |
| <b>switchport port-security mac-address</b>       | Sets the static secure address.                                |
| <b>switchport port-security aging</b>             | Sets the aging time for secure address.                        |

**Platform** N/A

**Description**

## 4.4 switchport port-security interface binding

Use these commands to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded.

Use the **no** form of these commands to remove the binding addresses.

**switchport port-security interface** *interface-id* **binding** [ *mac-address* **vlan** *vlan\_id* ] *ipv4-address*

**no switchport port-security interface** *interface-id* **binding** [ *mac-address* **vlan** *vlan\_id* ]

*ipv4-address*

#### Parameter Description

| Parameter                            | Description                               |
|--------------------------------------|-------------------------------------------|
| <b>interface</b> <i>interface-id</i> | <b>Binds interface ID.</b>                |
| <i>mac-address</i>                   | Binds source MAC address.                 |
| <b>vlan</b> <i>vlan_id</i>           | VLAN ID of the binding source MAC address |
| <i>ipv4-address</i>                  | Binds IPv4 address.                       |

**Defaults** N/A

**Command** Global configuration mode

**Mode**

- Usage Guide**
1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses.
  2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.

**Configuration** The following example binds the IP address 192.168.1.100 on the interface g 0/10.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 binding
192.168.1.100
Ruijie(config)# end
```

The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on the interface g 0/10.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 binding
00d0.f800.5555 vlan 1 192.168.1.100
Ruijie(config)# end
```

**Related Commands**

| Command                                     | Description                                                            |
|---------------------------------------------|------------------------------------------------------------------------|
| <b>show port-security</b>                   | Displays port security settings.                                       |
| <b>switchport port-security</b>             | Enables the port-security.                                             |
| <b>switchport port-security binding</b>     | Configures the secure address binding in interface configuration mode. |
| <b>switchport port-security mac-address</b> | Sets the static secure address.                                        |
| <b>switchport port-security aging</b>       | Sets the aging time for secure address.                                |

**Platform** N/A

**Description**

## 4.5 switchport port-security mac-address


Use this command to configure the static secure address.

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

**switchport port-security mac-address *mac-address* [ vlan *vlan-id* ]**

**no switchport port-security mac-address *mac-address* [ vlan *vlan-id* ]**

**Parameter Description**

| Parameter          | Description                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>mac-address</i> | Static secure MAC address                                                                                                                              |
| <i>vlan-id</i>     | VLAN ID of the MAC address                                                                                                                             |
|                    |  The configuration of <i>vlan-id</i> is only supported on the TRUNK |

|  |       |
|--|-------|
|  | port. |
|--|-------|

**Defaults** N/A

**Command Mode** Interface configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if-GigabitEthernet 0/10)# switchport port-security mac-address 00d0.f800.5555 vlan 2
Ruijie(config-if-GigabitEthernet 0/10)# end
```

| Related Commands | Command                                               | Description                                             |
|------------------|-------------------------------------------------------|---------------------------------------------------------|
|                  | <b>show port-security</b>                             | Displays port security settings.                        |
|                  | <b>switchport port-security</b>                       | Enables the port-security.                              |
|                  | <b>switchport port-security binding</b>               | Configures the secure address binding.                  |
|                  | <b>switchport port-security mac-address interface</b> | Sets the static secure address in privileged EXEC mode. |
|                  | <b>switchport port-security aging</b>                 | Sets the aging time for the secure address.             |

**Platform Description** N/A

## 4.6 switchport port-security interface mac-address


Use this command to configure the static secure address.

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

**switchport port-security interface** *interface-id* **mac-address** *mac-address* [ **vlan** *vlan-id* ]

**no switchport port-security interface** *interface-id* **mac-address** *mac-address* [ **vlan** *vlan-id* ]

| Parameter Description | Parameter                             | Description                |
|-----------------------|---------------------------------------|----------------------------|
|                       | <b>interface</b> <i>interface-id</i>  | Interface ID               |
|                       | <b>mac-address</b> <i>mac-address</i> | Static secure address      |
|                       | <b>vlan</b> <i>vlan-id</i>            | VLAN ID of the MAC address |

 The configuration of *vlan-id* is only supported on the TRUNK

|  |       |
|--|-------|
|  | port. |
|--|-------|

**Defaults** N/A

**Command Mode** Global configuration mode

**Usage Guide** N/A

**Configuration Examples** The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively.

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security interface g0/10 mac-address
00d0.f800.5555 vlan 2
Ruijie(config)# end
```

**Related Commands**

| Command                                     | Description                                                     |
|---------------------------------------------|-----------------------------------------------------------------|
| <b>show port-security</b>                   | Displays port security settings.                                |
| <b>switchport port-security</b>             | Enables the port-security.                                      |
| <b>switchport port-security binding</b>     | Configures the secure address binding.                          |
| <b>switchport port-security mac-address</b> | Sets the static secure address in interface configuration mode. |
| <b>switchport port-security aging</b>       | Sets the aging time for the secure address.                     |

**Platform** N/A

**Description**

## 4.7 show port-security

Use this command to display the port security configuration and the secure address.

**show port-security** [ **address** [ **interface** *interface-id* ] | **binding** [ **interface** *interface-id* ] | **interface** *interface-id* | **all** ]

**Parameter Description**

| Parameter                            | Description                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------|
| <b>address</b>                       | Displays all secure addresses, or the secure address of the specified port.               |
| <b>binding</b>                       | Displays all port security bindings, or the port security bindings of the specified port. |
| <b>interface</b> <i>interface-id</i> | Displays the port security configuration of the specified port.                           |
| <b>all</b>                           | Displays all valid secure addresses and valid port security bindings.                     |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Usage Guide** To display all port security configuration and violation management, execute the command without any parameter. To display the security configuration, the secure address, or the port security binding of the specified interface, execute the command with the corresponding parameter.

**Configuration Examples** The following example displays the port security statistics.

```
Ruijie#show port-security
NO. SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind
SecurityAction AgingTime
 (Count) (Count) (Count) (Count)
(min)

1 Gi0/1 128 2 2 1 protect
0

Total secure addresses in System : 2
Total secure bindings in System : 3
```

| Field                            | Description                                                |
|----------------------------------|------------------------------------------------------------|
| NO.                              | Serial number.                                             |
| Secure Port                      | Port name                                                  |
| MaxSecureAddr(count)             | The maximum number of secure addresses on the port.        |
| CurrentAddr(count)               | The current number of secure addresses on the port.        |
| CurrentIpBind (count)            | The current number of IP addresses bindings on the port.   |
| CurrentIpMacBind (count)         | The current number of IP-MAC address bindings on the port. |
| Security Action                  | Violation management.                                      |
| AgingTime                        | Aging time                                                 |
| Total secure addresses in System | The total number of secure addresses on the device.        |
| Total secure bindings in System  | The total number of port security bindings on the device,  |

The following example displays the port security configuration on interface GigabitEthernet 0/1.

```
Ruijie#show port-security interface gigabitEthernet 0/1
```



```

Interface : GigabitEthernet 0/1
Port status : down
Port Security : enabled
SecureStatic address aging : disabled
Sticky dynamic address : disabled
Violation mode : protect
Maximum MAC Addresses : 128
Total MAC Addresses : 2
Configured MAC Addresses : 2
Dynamic MAC Addresses : 0
Sticky MAC Addresses : 0
Total security binding : 3
IPv4-ONLY Binding Addresses : 1
IPv6-ONLY Binding Addresses : 1
IPv4-MAC Binding Addresses : 1
IPv6-MAC Binding Addresses : 0
Aging time(min) : 0

```

| Field                       | Description                                                                            |
|-----------------------------|----------------------------------------------------------------------------------------|
| Interface                   | Port name.                                                                             |
| Port status                 | Port status.                                                                           |
| Port Security               | Displays whether the port security is enabled.                                         |
| SecureStatic address aging  | Displays whether the static secure address aging is enabled.                           |
| Sticky dynamic address      | Displays whether the dynamic secure address is converted to the sticky secure address. |
| Violation mode              | Port violation management.                                                             |
| Maximum MAC Addresses       | The maximum number of secure addresses on the port.                                    |
| Total MAC Addresses         | The number of valid secure addresses on the port.                                      |
| Configured MAC Addresses    | The number of static secure addresses.                                                 |
| Dynamic MAC Addresses       | The number of dynamic secure addresses.                                                |
| Sticky MAC Addresses        | The number of sticky secure addresses.                                                 |
| Total security binding      | The number of valid port security bindings.                                            |
| IPv4-ONLY Binding Addresses | The number of IPv4 addresses bindings.                                                 |
| IPv6-ONLY Binding Addresses | The number of IPv6 addresses bindings.                                                 |
| IPv4-MAC Binding Addresses  | The number of IPv4-MAC address bindings.                                               |
| IPv6-MAC Binding Addresses  | The number of IPv6-MAC address bindings.                                               |
| Aging time(min)             | The aging time of the secure address.                                                  |

The following example displays all secure addresses on the device.

```

Ruijie#show port-security address
NO. VLAN MacAddress PORT TYPE

```

```

RemainingAge (mins) STATUS

1 1 00d0.f800.073c GigabitEthernet 0/1 Configured --
active
2 1 00d0.f800.073d GigabitEthernet 0/1 Configured --
active

```

| Field               | Description                           |
|---------------------|---------------------------------------|
| NO.                 | Serial number.                        |
| Vlan                | VLAN ID.                              |
| Mac Address         | MAC address.                          |
| Port                | Port name.                            |
| Type                | Secure address type.                  |
| Remaining Age(mins) | The aging time of the secure address. |
| STATUS              | The secure address status.            |

The following example displays all port security bindings on the device.

```

Ruijie#show port-security binding
NO. VLAN MacAddress PORT IpAddress
FilterType FilterStatus

1 1 00d0.f800.073c Gi0/1 192.168.12.202
ipv4-mac active
2 -- -- Gi0/1 192.168.0.1
ipv4-only active
3 -- -- Gi0/1 ffaa:ddcc::1
ipv6-only active

```

| Field        | Description                                      |
|--------------|--------------------------------------------------|
| NO.          | Serial number.                                   |
| Vlan         | VLAN ID.                                         |
| Mac Address  | MAC address.                                     |
| Port         | Port name.                                       |
| IpAddress    | IP address.                                      |
| FilterType   | The filtering type of the port security binding. |
| FilterStatus | The status of the port security binding.         |

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description**

N/A

## 5 SSH Commands

### 5.1 crypto key generate

Use this command to generate a public key to the SSH server.

**crypto key generate { rsa | dsa }**




| Parameter   | Parameter | Description           |
|-------------|-----------|-----------------------|
| Description | rsa       | Generates an RSA key. |
|             | dsa       | 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**

```
Ruijie# configure terminal
Ruijie(config)# crypto key generate rsa
```

| Related Commands | Command                          | Description                                                    |
|------------------|----------------------------------|----------------------------------------------------------------|
|                  | show ip ssh                      | Displays the current status of the SSH server.                 |
|                  | crypto key zeroize { rsa   dsa } | Deletes DSA and RSA keys and disables the SSH server function. |

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

## 5.2 crypto key zeroize

Use this command to delete a public key to the SSH server.

**crypto key zeroize { rsa | dsa }**

|                    | Parameter  | Description          |
|--------------------|------------|----------------------|
| <b>Parameter</b>   |            |                      |
| <b>Description</b> | <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**

```
Ruijie# configure terminal
Ruijie(config)# crypto key zeroize rsa
```

|                         | Command                                  | Description                                    |
|-------------------------|------------------------------------------|------------------------------------------------|
| <b>Related Commands</b> | <b>show ip ssh</b>                       | Displays the current status of the SSH server. |
|                         | <b>crypto key generate { rsa   dsa }</b> | Generates DSA and RSA keys.                    |

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

## 5.3 disconnect ssh

Use this command to disconnect the established SSH connection.

**disconnect ssh [ vty ] session-id**

|                    | Parameter         | Description                                                     |
|--------------------|-------------------|-----------------------------------------------------------------|
| <b>Parameter</b>   |                   |                                                                 |
| <b>Description</b> | <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.

```
Ruijie# disconnect ssh 1
```

The following example disconnects the established SSH connection by specifying the VTY session ID.

```
Ruijie# 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 Description** N/A

## 5.4 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          | Description                                     |
|--------------------|-------------------------------------------------|
| <b>retry-times</b> | Authentication retry times, ranging from 0 to 5 |

**Defaults** The default is 3.

**Command Mode** Global configuration 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 Examples** The following example sets the authentication retry times to 2.

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip ssh authentication-retries 2
```

| Related Commands | Command                  | Description                                    |
|------------------|--------------------------|------------------------------------------------|
|                  | <code>show ip ssh</code> | Displays the current status of the SSH server. |

**Platform** N/A

**Description**

## 5.5 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          | Parameter     | Description                                                                                                                                   |
|--------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Description</b> | <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** ctr encryption mode is 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**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

**Platform** N/A

**Description**

## 5.6 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       |
|-------------|----------------|-------------------|
| Description | <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: Not support  
SSHv2: Support SHA1

**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**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

**Platform** N/A

**Description**

## 5.7 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** The following example sets RSA and DSA key files associated with user **test**.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

| Related Commands | Command            | Description                                    |
|------------------|--------------------|------------------------------------------------|
|                  | <b>show ip ssh</b> | Displays the current status of the SSH server. |

**Platform Description** N/A

## 5.8 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 Description | Parameter   | 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**

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

| Related Commands | Command            | Description                                    |
|------------------|--------------------|------------------------------------------------|
|                  | <b>show ip ssh</b> | Displays the current status of the SSH server. |



**Platform** N/A

**Description**

## 5.9 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                                  |
|--------------------|-----------|----------------------------------------------|
| <b>Description</b> | <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**

```
Ruijie# configure terminal
Ruijie(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**

## 5.10 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           |
|--------------------|------------|-----------------------|
| <b>Description</b> | <b>rsa</b> | Displays the RSA key. |

|            |                       |
|------------|-----------------------|
| <b>dsa</b> | Displays the DSA key. |
|------------|-----------------------|

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration 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.

```
Ruijie# 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                 |
|-----------------|------------------------------------------------|-----------------------------|
| <b>Commands</b> | <code>crypto key generate { rsa   dsa }</code> | Generates DSA and RSA keys. |

**Platform Description** N/A

### 5.11 show ip ssh

Use this command to display the information of the SSH server.

**show ip ssh**

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

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration mode

**Usage Guide** This command is used to display the information of the SSH server, including version, enablement state, authentication timeout, and authentication retry times.  
 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:
Ruijie# show ip ssh
SSH Disable - version 1.99
please enable service ssh-server
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

SSH and SCP enabled:
Ruijie# show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

```

| Field                           | Description                                   |
|---------------------------------|-----------------------------------------------|
| SSH Enable/Disable              | Whether SSH is enabled or disabled.           |
| Authentication timeout          | Timeout of user authentication                |
| Authentication retries          | Retry times of user authentication            |
| SSH SCP Server enabled/disabled | Whether SSH SCP server is enabled or disabled |

| 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 Description** N/A

## 5.12 show ssh

Use this command to display the information about the established SSH connection.

**show ssh**

| Parameter   | Parameter | Description |
|-------------|-----------|-------------|
| Description | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode/Global configuration 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 Examples** The following example displays the information about the established SSH connection:

```
Ruijie# 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                      |
|------------|----------------------------------|
| 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 Description** N/A

## 6 CPU Protection Commands

### 6.1 clear cpu-protect counters

Use this command to clear the CPP statistics.

**clear cpu-protect counters**

| <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 clears the CPP statistics.

```
Ruijie#clear cpu-protect counters
```

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

**Platform Description** N/A

### 6.2 show cpu-protect

Use this command to display all CPP configuration and statistics.

**show cpu-protect**

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

**Defaults** N/A

**Command Mode** All configuraiton mode

**Usage Guide** N/A

**Configuration** Ruijie(config)#show cpu-protect type bpdu

**Examples** %cpu port bandwidth: 1000(pps)

```

Traffic-class Bandwidth(pps) Rate(pps) Drop(pps)

0 100 0 0
1 100 1 0
2 1000 0 0
3 1000 0 0
4 1000 0 0
5 1000 0 0
6 1000 0 0
7 1000 0 0

Packet Type Traffic-class Bandwidth(pps) Rate(pps) Drop(pps)
Total Total Drop

arp 1 100 1 0 34176
65
dhcp 2 300 0 0 568
0
da-lookup-miss 0 100 0 0 0
0
dvmrp 2 100 0 0 0
0
igmp 2 256 0 0 0
0
pim 2 128 0 0 0
0
local 3 1000 0 0 27879
0
other 0 100 0 0 7636
0
12-packet 6 300 0 0 477506
0

```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |


**Platform Description** N/A

## 7 DHCP Snooping Commands

### 7.1 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* ]

| <b>Parameter Description</b>  | 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.                |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                                                                                                                                            |                                                                 |
| <b>Command Mode</b>           | Privileged EXEC mode                                                                                                                                                                                                                                                                                                           |                                                                 |
| <b>Usage Guide</b>            | Use this command to clear the current dynamic user information from the DHCP Snooping binding database.                                                                                                                                                                                                                        |                                                                 |
|                               | <p> 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.</p>                                                      |                                                                 |
| <b>Configuration Examples</b> | <p>The following example clears the dynamic database information from the DHCP Snooping binding database.</p> <pre>Ruijie# clear ip dhcp snooping binding Ruijie# show ip dhcp snooping binding Total number of bindings: 0 NO.    MACADDRESS      IPADDRESS      LEASE (SEC)   TYPE          VLAN INTERFACE ----- -----</pre> |                                                                 |
| <b>Related Commands</b>       | Command                                                                                                                                                                                                                                                                                                                        | Description                                                     |
|                               | <b>show ip dhcp snooping binding</b>                                                                                                                                                                                                                                                                                           | Displays the information of the DHCP Snooping binding database. |

**Platform** N/A

**Description**

## 7.2 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.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping
Ruijie(config)# end
```

| 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** N/A

**Description**

## 7.3 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<br>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**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping bootp-bind
Ruijie(config)# end
```

| Related<br>Commands | Command                      | Description                               |
|---------------------|------------------------------|-------------------------------------------|
|                     | <b>show ip dhcp snooping</b> | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 7.4 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<br>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 Examples** The following example enables DHCP Snooping to support the function of processing Relay requests.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping check-giaddr
Ruijie(config)# end
```

**Related Commands**

| Command                      | Description                                                  |
|------------------------------|--------------------------------------------------------------|
| <b>show ip dhcp snooping</b> | Displays the configuration information of the DHCP Snooping. |

**Platform** N/A

**Description**

## 7.5 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** The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-delay 3600
Ruijie(config)# end
```

**Related Commands**

| Command                      | Description                                                  |
|------------------------------|--------------------------------------------------------------|
| <b>show ip dhcp snooping</b> | Displays the configuration information of the DHCP Snooping. |

**Platform** N/A

**Description**

## 7.6 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       | 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 into flash.

**Configuration** The following example writes the dynamic user information of the DHCP binding database into flash.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping database write-to-flash
Ruijie(config)# end
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 7.7 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 ]**

**no ip dhcp snooping information option [ standard-format ]**


| Parameter Description | Parameter              | Description                            |
|-----------------------|------------------------|----------------------------------------|
|                       | <b>standard-format</b> | The option82 uses the standard format. |

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

**Command Mode** Global configuration 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

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
```

| Related Commands | Command                      | Description                               |
|------------------|------------------------------|-------------------------------------------|
|                  | <b>show ip dhcp snooping</b> | Displays the DHCP Snooping configuration. |

**Platform Description** N/A

## 7.8 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**

| Parameter | Parameter | Description |
|-----------|-----------|-------------|
|-----------|-----------|-------------|

|                    |                                   |                                                                                        |
|--------------------|-----------------------------------|----------------------------------------------------------------------------------------|
| <b>Description</b> |                                   |                                                                                        |
|                    | <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 Examples** The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option format remote-id hostname
```

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

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

## 7.9 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**

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

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

**Command** Interface configuration mode  
**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 0/2 to be in the suppression status.

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip dhcp snooping suppression
Ruijie(config-if-GigabitEthernet 0/2)# end
```

**Related  
Commands**

| Command                      | Description                               |
|------------------------------|-------------------------------------------|
| <b>show ip dhcp snooping</b> | Displays the DHCP Snooping configuration. |

**Platform** N/A

**Description**

## 7.10 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** The following example sets GigabitEthernet 0/1 as a trusted port:

**Examples**

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/1)# end
```

| Related Commands | Command | Description                  |
|------------------|---------|------------------------------|
|                  |         | <b>show ip dhcp snooping</b> |

**Platform** N/A

**Description**

## 7.11 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.

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping verify mac-address
Ruijie(config)# end
```

| Related Commands | Command | Description                  |
|------------------|---------|------------------------------|
|                  |         | <b>show ip dhcp snooping</b> |

**Platform** N/A

**Description**

## 7.12 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> | VLAN range of effective DHCP Snooping   |
|                       | <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**

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

| Related Commands | Command                 | Description                     |
|------------------|-------------------------|---------------------------------|
|                  | <b>ip dhcp snooping</b> | Enables DHCP Snooping globally. |

**Platform** N/A

**Description**

## 7.13 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**

| 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 Examples** The following adds the option82 to the DHCP request packets and changes the VLAN 4094 in the option82 sub-option circuit-id to VLAN93:

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information
option change-vlan-to vlan 4093
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 7.14 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**

**Parameter Description**

| Parameter           | Description                                        |
|---------------------|----------------------------------------------------|
| <i>vlan-id</i>      | The VLAN where the DHCP request packets are        |
| <i>ascii-string</i> | The user-defined content to fill to the Circuit ID |

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

**Command** Interface configuration mode  
**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 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*.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information
option format-type circuit-id string port-name
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform Description** N/A

## 7.15 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>   | VLAN range                                                                   |
| <i>user-number</i> | The maximum number of users bound with the VLAN, in the range from 1 to 255. |

**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.

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitethernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user
30
Ruijie(config-if-GigabitEthernet 0/1)# end
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 7.16 renew ip dhcp snooping database

Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.


**renew ip dhcp snooping database****Parameter  
Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** N/A

**Command  
Mode** Privileged EXEC mode

**Usage Guide** This command is used to import the flash 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 flash file information to the DHCP Snooping database.

**Examples** Ruijie# renew ip dhcp snooping database

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 7.17 show ip dhcp snooping

Use this command to display the DHCP Snooping configuration.

**show ip dhcp snooping**

| Parameter Description | Parameter | Description |
|-----------------------|-----------|-------------|
|                       | N/A       | N/A         |

**Defaults** N/A

**Command Mode** Privileged EXEC mode

**Mode**

**Usage Guide** N/A

**Configuration Examples** The following example displays the DHCP Snooping configuration.

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping status : DISABLE
DHCP snooping Verification of hwaddr status : DISABLE
DHCP snooping database write-delay time : 0 seconds
DHCP snooping option 82 status : DISABLE
DHCP snooping Support bootp bind status : DISABLE

Interface Trusted Rate limit (pps)

Default No unlimited
```

| 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**

## 7.18 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** The following example displays the information of the DHCP Snooping binding database.

### Examples

```
Ruijie# 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
```

| 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.                            |
| INTERFACE                | The user's connection interface.                            |

### Related Commands

| Command                               | Description                                                     |
|---------------------------------------|-----------------------------------------------------------------|
| <b>ip dhcp snooping binding</b>       | Adds the static user information to the DHCP Snooping database. |
| <b>clear ip dhcp snooping binding</b> | Clears the dynamic user information from the                    |

|  |                                 |
|--|---------------------------------|
|  | DHCP Snooping binding database. |
|--|---------------------------------|

**Platform** N/A

**Description**

## 8 ACL Commands

### 8.1 command ID table

For IDs used in the following commands, refer to the command ID table below:

| ID                         | Meaning                                                                                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID                         | Number of access list. Range:<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                                                                                                                                         |
| name                       | ACL name                                                                                                                                                                                                                                                                                    |
| sn                         | ACL SN (products can be set according to the priority)                                                                                                                                                                                                                                      |
| start-sn                   | Start sequence number                                                                                                                                                                                                                                                                       |
| inc-sn                     | Sequence number increment                                                                                                                                                                                                                                                                   |
| deny                       | If matched, access is denied.                                                                                                                                                                                                                                                               |
| permit                     | If matched, access is permitted.                                                                                                                                                                                                                                                            |
| port                       | Protocol number. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP,AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually. |
| source                     | Packet source IP address (host address or network address)                                                                                                                                                                                                                                  |
| source-wildcard            | Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.                                                                                                                                                                                                               |
| dscp                       | Differential service code point, and code point value. Range: 0 to 63                                                                                                                                                                                                                       |
| destination                | Packet destination IP address (host address or network address)                                                                                                                                                                                                                             |
| destination-wildcard       | Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32                                                                                                                                                                                                                |
| fragment                   | Packet fragment filtering.                                                                                                                                                                                                                                                                  |
| precedence                 | Packet precedence value (0 to 7)                                                                                                                                                                                                                                                            |
| time-range time-range-name | Time range of packet filtering, named <i>tm-rng-name</i>                                                                                                                                                                                                                                    |
| tos                        | Type of service (0 to 15)                                                                                                                                                                                                                                                                   |
| icmp-type                  | ICMP message type (0 to 255)                                                                                                                                                                                                                                                                |
| icmp-code                  | ICMP message type code (0 to 255)                                                                                                                                                                                                                                                           |
| icmp-message               | ICMP message type name (0 to 255)                                                                                                                                                                                                                                                           |
| operator port [ port ]     | Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range)<br><i>port</i> indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number                                                                                    |

|                      |                                                  |
|----------------------|--------------------------------------------------|
| source-mac-addr      | Physical address of the source host              |
| destination-mac-addr | Physical address of the destination host         |
| ethernet-type        | Ethernet protocol type. 0x value can be entered. |
| match-all tcpf       | Match all bits of the TCP flag.                  |
| established          | Match the RST or ACK bit of the TCP flag.        |
| in                   | Filter the incoming packets of the interface     |
| out                  | Filter the outgoing packets of the interface     |

## 8.2 access-list

Use this command to create an access list to filter data packets. Use the **no** form of this command to remove the specified access list.

- Standard IP access list (1 to 99, 1300 to 1999)

**access-list** *acl-id* { **deny** | **permit** } { *source source-wildcard* | **any** | **host source** } [ **time-range** *tm-range-name* ]

- Extended IP access list (100 to 199, 2000 to 2699)

**access-list** *acl-id* { **deny** | **permit** } *protocol* { *source source-wildcard* | **any** | **host source** } [ *operator port* [ *port* ] ] { *destination destination-wildcard* | **any** | **host destination** } [ *operator port* [ *port* ] ] [ [ **precedence** *precedence* ] [ **tos** *tos* ] | [ **dscp** *dscp* ] [ **fragment** ] [ **time-range** *time-range-name* ]

- Extended MAC access list (700 to 799)

**access-list** *acl-id* { **deny** | **permit** } { *source-mac-address mask* | **any** | **host source-mac-address** } { *destination-mac-address mask* | **any** | **host destination-mac-address** } [ *ethernet-type* ] [ **time-range** *time-range-name* ]

### 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, 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>      | It 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>fragment</b>             | Packet fragment filtering                                                                                                                                                                                                                              |



|                                     |                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------|
| <b>precedence</b>                   | Specify the packet priority.                                                                       |
| <i>precedence</i>                   | Packet precedence value (0 to 7)                                                                   |
| <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.                                                             |
| <b>time-range</b>                   | Time range of packet filtering                                                                     |
| <i>time-range-name</i>              | Time range name of packet filtering                                                                |
| <b>tos</b>                          | Specify type of service.                                                                           |
| <i>tos</i>                          | ToS value (0 to 15)                                                                                |
| <b>dscp</b>                         | Differentiated service code point                                                                  |
| <i>dscp</i>                         | Code point value, ranging from 0 to 63                                                             |
| <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)                              |
| <i>port [ port ]</i>                | Port number; <i>range</i> needs two port numbers, while other operators only need one port number. |
| <b>host source-mac-address</b>      | Source physical address                                                                            |
| <b>host destination-mac-address</b> | Destination physical address                                                                       |
| <i>ethernet-type</i>                | Ethernet type                                                                                      |
| <b>match-all</b>                    | Match all the bits of the TCP flag.                                                                |
| <i>tcp-flag</i>                     | Match the TCP flag.                                                                                |
| <b>established</b>                  | Match the RST or ACK bits, not other bits of the TCP flag.                                         |

**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 extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type.

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
- lavc-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

 Run **no { sn | permit | deny }** in ACL mode to delete ACEs.

**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:

```
Ruijie (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:

```
Ruijie(config)#access-list 102 permit tcp any any eq domain log
Ruijie(config)#access-list 102 permit udp any any eq domain log
Ruijie(config)#access-list 102 permit icmp any any echo log
Ruijie(config)#access-list 102 permit icmp any any echo-reply
```

3. Example of the extended MAC ACL

This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 0/1. The configuration procedure is as below:

```
Ruijie(config)#access-list 702 deny host 00d0f8000c0c any aarp
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mac access-group 702 in
```

**Related  
Commands**

| Command                  | Description                                  |
|--------------------------|----------------------------------------------|
| <b>show access-lists</b> | Show all the ACLs.                           |
| <b>mac access-group</b>  | Apply the extended MAC ACL on the interface. |

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

### 8.3 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 tm-range-name]
```

2. Extended IP ACL

```
[sn] deny protocol { source source-wildcard | any | host source } [operator port [port]] { destination destination-wildcard | any | host destination } [operator port [port]] [[precedence precedence] [tos tos]] [[dscp dscp]] [fragment] [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 | any | host source } { destination destination-wildcard | any | host destination } [icmp-type] [[icmp-type [icmp-code]]] [[icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]
```

- Transmission Control Protocol (TCP)


```
[sn] deny tcp { source source-wildcard | any | host source } [operator port [port]] { destination destination-wildcard | any | host destination } [operator port [port]] [[precedence precedence] [tos tos]] [[dscp dscp]] [fragment] [time-range time-range-name] [match-all tcp-flag | established]
```

- User Datagram Protocol (UDP)

```
[sn] deny udp { source source-wildcard | any | host source } [operator port [port]] { destination destination-wildcard | any | host destination } [operator port [port]] [[precedence precedence] [tos tos]] [[dscp dscp]] [fragment] [time-range time-range-name]
```

3. Extended MAC ACL

```
[sn] deny { source-mac-address mask | any | host source-mac-address } { destination-mac-address mask | any | host destination-mac-address } [ethernet-type] [time-range time-range-name]
```

 For ACL associated with address pool, if there is not IP address, this entry will not be delivered.

Parameter Description

| Parameter              | Description                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>sn</i>              | ACL entry sequence number                                                                                                                                                                                                                              |
| <b>deny</b>            | If not matched, access is denied.                                                                                                                                                                                                                      |
| <i>source</i>          | Specify the source IP address (host address or network address).                                                                                                                                                                                       |
| <i>source-wildcard</i> | It 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>fragment</b>                            | Packet fragment filtering                                                                          |
| <b>precedence</b>                          | Specify the packet priority.                                                                       |
| <i>precedence</i>                          | Packet precedence value (0 to 7)                                                                   |
| <b>time-range</b>                          | Time range of packet filtering                                                                     |
| <i>time-range-name</i>                     | Time range name of packet filtering                                                                |
| <b>tos</b>                                 | Specify type of service.                                                                           |
| <i>tos</i>                                 | ToS value (0 to 15)                                                                                |
| <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)                              |
| <i>port [ port ]</i>                       | Port number; <i>range</i> needs two port numbers, while other operators only need one port number. |
| <b>host</b> <i>source-mac-address</i>      | Source physical address                                                                            |
| <b>host</b> <i>destination-mac-address</i> | Destination physical address                                                                       |
| <i>ethernet-type</i>                       | Ethernet type                                                                                      |
| <b>match-all</b>                           | Match all the bits of the TCP flag.                                                                |
| <i>tcp-flag</i>                            | Match the TCP flag.                                                                                |
| <b>established</b>                         | Match the RST or ACK bits, not other bits of the TCP flag.                                         |
| <b>dscp</b>                                | Differential Service Code Point                                                                    |
| <i>dscp</i>                                | Code value, within the range of 0 to 63                                                            |

**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** 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:

```
Ruijie(config)# ip access-list extended ip-ext-acl
Ruijie(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#ip access-group ip-ext-acl in
```

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:

```
Ruijie(config)#mac access-list extended mac1
Ruijie(config-mac-nacl)#deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(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:

```
Ruijie(config)#ip access-list standard 34
Ruijie(config-ext-nacl)# deny host 192.168.4.12
Ruijie(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Ruijie(config-ext-nacl)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip access-group 34 in
```

#### Related Commands

| Command                  | Description                                    |
|--------------------------|------------------------------------------------|
| <b>show access-lists</b> | Displays all ACLs.                             |
| <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>permit</b>            | Permits the access.                            |

**Platform** N/A

**Description**

## 8.4 ip access-group

Use this command to apply a specific access list globally or to an interface. Use the **no** form of this command to remove the access list from the interface.

```
ip access-group { acl-id | acl-name } in
no ip access-group { acl-id | acl-name } in
```



| 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.                              |

**Defaults** No access list is applied globally or on the interface by default.

**Command mode** Global configuration mode, interface configuration mode.

**Usage Guide** Use this command to control access to a specified interface or globally.

**Configuration Examples** The following example applies the ACL 120 on interface GigabitEthernet0/1 to filter the incoming packets:

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(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. |

**Platform** N/A

**Description**

## 8.5 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** The following example creates a standard access list named std-acl.

**Examples**

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
Ruijie(config-std-nacl)#
```

The following example creates an extended ACL numbered 123:

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 123
```

**Related Commands**

| Command                  | Description        |
|--------------------------|--------------------|
| <b>show access-lists</b> | Displays all ACLs. |

**Platform Description** N/A

## 8.6 mac access-group

Use this command to apply the specified MAC access list globally or 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**  
**no mac access-group** { *acl-id* | *acl-name* } **in**

**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.           |

**Defaults** No MAC access list is applied by default.

| <b>Command</b>                 | Global configuration mode, interface configuration mode.                                                                                                                                                                    |         |             |                                |                                                  |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------|--------------------------------|--------------------------------------------------|
| <b>mode</b>                    |                                                                                                                                                                                                                             |         |             |                                |                                                  |
| <b>Usage Guide</b>             | Use this command to apply the access list globally or to the interface to filter the inbound or outbound packets based on the MAC address.                                                                                  |         |             |                                |                                                  |
| <b>Configuration Examples</b>  | The following example applies the MAC access-list <code>accept_00d0f8xxxxxx_only</code> to interface GigabitEthernet 0/1:                                                                                                   |         |             |                                |                                                  |
|                                | <pre>Ruijie(config)# interface GigaEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# mac access-group accept_00d0f8xxxxxx_only in</pre>                                                                                   |         |             |                                |                                                  |
| <b>Related Commands</b>        | <table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><code>show access-group</code></td> <td>Displays the ACL configuration on the interface.</td> </tr> </tbody> </table> | Command | Description | <code>show access-group</code> | Displays the ACL configuration on the interface. |
| Command                        | Description                                                                                                                                                                                                                 |         |             |                                |                                                  |
| <code>show access-group</code> | Displays the ACL configuration on the interface.                                                                                                                                                                            |         |             |                                |                                                  |
| <b>Platform</b>                | N/A                                                                                                                                                                                                                         |         |             |                                |                                                  |
| <b>Description</b>             |                                                                                                                                                                                                                             |         |             |                                |                                                  |

## 8.7 mac access-list extended

Use this command to create an extended MAC 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* }

| <b>Parameter Description</b>  | <table border="1"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>acl-id</i></td> <td>Extended MAC access list number. The range is from 700 to 799.</td> </tr> <tr> <td><i>acl-name</i></td> <td>Name of the extended MAC access list</td> </tr> </tbody> </table> | 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 extended MAC access list |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|---------------|----------------------------------------------------------------|-----------------|--------------------------------------|
| 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 extended MAC access list                                                                                                                                                                                                                                                                         |           |             |               |                                                                |                 |                                      |
| <b>Defaults</b>               | N/A                                                                                                                                                                                                                                                                                                          |           |             |               |                                                                |                 |                                      |
| <b>Command mode</b>           | Global configuration mode.                                                                                                                                                                                                                                                                                   |           |             |               |                                                                |                 |                                      |
| <b>Usage Guide</b>            | To filter the packets based on the MAC address, you need to define a MAC access list by using the <b>mac access-list extended</b> command.                                                                                                                                                                   |           |             |               |                                                                |                 |                                      |
| <b>Configuration Examples</b> | The following command creates an extended MAC access list named <code>mac-acl</code> :                                                                                                                                                                                                                       |           |             |               |                                                                |                 |                                      |
|                               | <pre>Ruijie(config)# mac access-list extended mac-acl Ruijie(config-mac-nacl)# show access-lists mac access-list extended mac-acl</pre>                                                                                                                                                                      |           |             |               |                                                                |                 |                                      |

The following command creates an extended MAC access list numbered 704:

```
Ruijie(config)# mac access-list extended 704
Ruijie(config-mac-nacl)# show access-lists mac access-list extended 704
```

#### Related Commands

| Command                  | Description                |
|--------------------------|----------------------------|
| <b>show access-lists</b> | Displays all access lists. |

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

## 8.8 mac access-list resequence

Use this command to resequence an extended MAC 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 extended MAC 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** Use this command to change the order of the access entries.

**Configuration Examples** The following example resequences entries of extended MAC access list "mac-acl":

**Examples** Before the configuration:

```
Ruijie# show access-lists
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

After the configuration:

```
Ruijie# config
Ruijie(config)# mac access-list resequence exp-acl 21 43
```

```
Ruijie(config)# exit
Ruijie# 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**

## 8.9 no sn

Use this command to delete an entry of the ACL.

**no sn**

**Parameter  
Description**

| Parameter | Description                      |
|-----------|----------------------------------|
| <i>sn</i> | Sequence number of the ACL entry |

**Defaults** N/A

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to delete an ACL entry in ACL configuration mode.

**Configuration**

```
Ruijie(config)# ip access-list standard acl
```

**Examples**

```
Ruijie(config-std-nacl)# 10 permit 192.168.1.0 0.0.0.255
Ruijie(config-std-nacl)# 20 permit host 192.168.2.100
Ruijie(config-std-nacl)# show access-lists acl
ip access-list standard acl
 10 permit 192.168.1.0 0.0.0.255
 20 permit host 192.168.2.100
Ruijie(config-std-nacl)# no 20
Ruijie(config-std-nacl)# show access-lists acl
ip access-list standard acl
 10 permit 192.168.1.0 0.0.0.255
Ruijie(config-std-nacl)#
```

**Related**

| Command | Description |
|---------|-------------|
|---------|-------------|

| Commands                 |                         |
|--------------------------|-------------------------|
| <b>show access-lists</b> | Show all the ACLs.      |
| <b>ip access-list</b>    | Define the IP ACL.      |
| <b>deny</b>              | Define the deny rule.   |
| <b>permit</b>            | Define the permit rule. |

**Platform** N/A

**Description**

## 8.10 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.

- Standard IP ACL

```
[sn] permit { source source-wildcard | any | host source } [time-range tm-range-name]
```

- Extended IP ACL

```
[sn] permit protocol { source source-wildcard | any | host source } [operator port [port]]
{ destination destination-wildcard | any | host destination } [operator port [port]] [[precedence
precedence] [tos tos] | [dscp dscp]] [fragment] [time-range time-range-name]
```

Extended IP ACLs of some important protocols:

Internet Control Message Protocol (ICMP)

```
[sn] permit icmp { source source-wildcard | any | host source } { destination destination-wildcard |
any | host destination } [icmp-type] [[icmp-type icmp-code]] | [icmp-message] [[precedence
precedence] [tos tos] | [dscp dscp]] [fragment] [time-range time-range-name]
```

Transmission Control Protocol (TCP)

```
[sn] permit tcp { source source-wildcard | any | host source } [operator port [port]] { destination
destination-wildcard | any | host destination } [operator port [port]] [[precedence precedence]
[tos tos] | [dscp dscp]] [fragment] [time-range time-range-name] [match-all tcp-flag |
established]
```

User Datagram Protocol (UDP)

```
[sn] permit udp { source source-wildcard | any | host source } [operator port [port]] { destination
destination-wildcard | any | host destination } [operator port [port]] [[precedence precedence]
[tos tos] | [dscp dscp]] [fragment] [time-range time-range-name]
```

- Extended MAC ACL

```
[sn] permit { source-mac-address mask | any | host source-mac-address } { destination
-mac-address mask | any | host destination-mac-address } [ethernet-type] [time-range
time-range-name]
```

 For ACL associated with address pool, if there is no IP address, this entry will not be delivered.

| Parameter Description | Parameter | Description               |
|-----------------------|-----------|---------------------------|
|                       | <i>sn</i> | ACL entry sequence number |

|                                            |                                                                                                                                                                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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>                     | It 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>fragment</b>                            | Packet fragment filtering                                                                                                                                                                                                                              |
| <b>precedence</b>                          | Specify the packet priority.                                                                                                                                                                                                                           |
| <i>precedence</i>                          | Packet precedence value (0 to 7)                                                                                                                                                                                                                       |
| <b>time-range</b>                          | Time range of packet filtering                                                                                                                                                                                                                         |
| <i>time-range-name</i>                     | Time range name of packet filtering                                                                                                                                                                                                                    |
| <b>tos</b>                                 | Specify type of service.                                                                                                                                                                                                                               |
| <i>tos</i>                                 | ToS value (0 to 15)                                                                                                                                                                                                                                    |
| <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)                                                                                                                                                                                  |
| <i>port [ port ]</i>                       | Port number; <i>range</i> needs two port numbers, while other operators only need one port number.                                                                                                                                                     |
| <b>host</b> <i>source-mac-address</i>      | Source physical address                                                                                                                                                                                                                                |
| <b>host</b> <i>destination-mac-address</i> | Destination physical address                                                                                                                                                                                                                           |
| <i>ethernet-type</i>                       | Ethernet type                                                                                                                                                                                                                                          |
| <b>match-all</b>                           | Match all the bits of the TCP flag.                                                                                                                                                                                                                    |
| <i>tcp-flag</i>                            | Match the TCP flag.                                                                                                                                                                                                                                    |
| <b>established</b>                         | Match the RST or ACK bits, not other bits of the TCP flag.                                                                                                                                                                                             |

**Defaults** N/A

**Command mode** ACL configuration mode.

**Usage Guide** Use this command to configure the **permit** conditions for the ACL in ACL configuration mode.

**Configuration Examples** 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:

```
Ruijie(config)# ip access-list extended 102
```

```
Ruijie(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip access-group 102 in
```

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:

```
Ruijie(config)#mac access-list extended 702
Ruijie(config-mac-nacl)#permit host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)#show access-lists
mac access-list extended 702
10 permit host 0013.0049.8272 any aarp 702
Ruijie(config-mac-nacl)#exit
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(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:

```
Ruijie(config)#ip access-list standard std-acl
Ruijie(config-std-nacl)#permit host 192.168.4.12
Ruijie(config-std-nacl)#show access-lists
ip access-list standard std-acl
 10 permit host 192.168.4.12
Ruijie(config-std-nacl)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip access-group std-acl in
```

#### Related Commands

| Command                  | Description                                            |
|--------------------------|--------------------------------------------------------|
| <b>show access-lists</b> | Displays all access lists.                             |
| <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>deny</b>              | Defines the <b>deny</b> access entry.                  |

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



## 8.11 show access-group

Use this command to display the access list applied to the interface.

**show access-group** [ **interface** *interface-name* ]

| Parameter Description | Parameter        | Description    |
|-----------------------|------------------|----------------|
|                       | <i>interface</i> | Interface name |

**Defaults** N/A

**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** Ruijie# show access-group

**Examples**

```
ip access-list standard ipstd3
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4
Applied On interface GigabitEthernet 0/2.
```

| 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. |

**Platform** N/A

**Description**

## 8.12 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         |
|                       | <i>acl-name</i> | Name of the IP access list |
|                       | <b>summary</b>  | Access list summary        |

**Defaults** N/A

**Command** Global configuration mode  
**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** Ruijie# show access-lists n\_acl

**Examples** ip access-list standard n\_acl

```
Ruijie# show access-lists 102
```

```
ip access-list extended 102
```

```
Ruijie# show access-lists
```

```
ip access-list standard n_acl
```

```
ip access-list extended 102
```

**Related  
Commands**

| Command                | Description                          |
|------------------------|--------------------------------------|
| <b>ip access-list</b>  | Defines an IP access list.           |
| <b>mac access-list</b> | Defines an extended MAC access list. |

**Platform** N/A

**Description**

## 8.13 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* ]**

**Parameter  
Description**

| Parameter        | Description    |
|------------------|----------------|
| <i>interface</i> | Interface name |

**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** Ruijie# show ip access-group interface gigabitethernet 0/1

**Examples** ip access-group aaa in

```
Applied On interface GigabitEthernet 0/1.
```

| <b>Related Commands</b> | Command                     | Description                |
|-------------------------|-----------------------------|----------------------------|
|                         | <code>ip access-list</code> | Defines an IP access list. |

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

## 8.14 show mac access-group

Use this command to display the MAC access list on the interface.

**show mac access-group [ interface *interface* ]**

| <b>Parameter Description</b> | Parameter        | Description    |
|------------------------------|------------------|----------------|
|                              | <i>interface</i> | Interface name |

**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**

```
Ruijie# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

| <b>Related Commands</b> | Command                      | Description                |
|-------------------------|------------------------------|----------------------------|
|                         | <code>mac access-list</code> | Defines a MAC access list. |

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

## 9 QoS Commands

### 9.1 mls qos cos

Use this command to configure the CoS value of an interface. Use the **no** or **default** form of this command to restore the default setting.

**mls qos cos** *default-cos*

**no mls qos cos**

**default mls qos cos**

| Parameter   | Parameter          | Description                                           |
|-------------|--------------------|-------------------------------------------------------|
| Description | <i>default-cos</i> | CoS value of the interface. The range is from 0 to 7. |

**Defaults** The default CoS value is 0.

**Command Mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures the default CoS value to 7.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mls qos cos 7
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     |             |

**Platform Description** N/A

### 9.2 mls qos map cos-dscp

Use this command to map the CoS value to the DSCP value. Use the **no** or **default** form of this command to restore the default CoS-DSCP mapping.

**mls qos map cos-dscp** *dscp1...dscp8*

**no mls qos map cos-dscp**

**default mls qos map cos-dscp**

| Parameter   | Parameter            | Description                                          |
|-------------|----------------------|------------------------------------------------------|
| Description | <i>dscp1...dscp8</i> | Specifies the DSCP value. The range is from 0 to 63. |

**Defaults** By default, the CoS 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

**Command** Global configuration mode

**Mode**

**Usage Guide** N/A

**Configuration**

```
Ruijie(config)# mls qos map cos-dscp 8 10 16 18 24 26 32 34
```

**Examples**

| Related         | Command                  | Description                    |
|-----------------|--------------------------|--------------------------------|
| <b>Commands</b> | <b>show mls qos maps</b> | Displays the CoS-DSCP mapping. |
|                 | <b>cos-dscp</b>          |                                |

**Platform** N/A

**Description**

### 9.3 mls qos map dscp-cos

Use this command to map the DSCP value to the CoS value. Use the **no** or **default** form of this command to restore the default DSCP-CoS mapping.

**mls qos map dscp-cos dscp-list to cos**

**no mls qos map dscp-cos**

**default mls qos map dscp-cos**

| Parameter          | Parameter        | Description                           |
|--------------------|------------------|---------------------------------------|
| <b>Description</b> | <i>dscp-list</i> | DSCP list. The range is from 0 to 63. |
|                    | <i>cos</i>       | CoS value. The range is from 0 to 7.  |

**Defaults** The default DSCP-CoS mapping is listed below:

|             |              |               |               |               |               |               |               |
|-------------|--------------|---------------|---------------|---------------|---------------|---------------|---------------|
| DSCP<br>0-7 | DSCP<br>8-15 | DSCP<br>16-23 | DSCP<br>24-31 | DSCP<br>32-39 | DSCP<br>40-47 | DSCP<br>48-55 | DSCP<br>56-63 |
| CoS 0       | CoS 1        | CoS 2         | CoS 3         | CoS 4         | CoS 5         | CoS 6         | CoS 7         |

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration**

```
Ruijie(config)# mls qos map dscp-cos 8 10 16 18 to 0
```

**Examples**

| Related  | Command                                     | Description                    |
|----------|---------------------------------------------|--------------------------------|
| Commands | <b>show mls qos maps</b><br><b>dscp-cos</b> | Displays the DSCP-CoS mapping. |

Platform N/A

Description

## 9.4 mls qos map ip-precedence-dscp

Use this command to map the IP precedence to the DSCP value. Use the **no** or **default** form of this command to restore the default IP-precedence to DSCP mapping.

**mls qos map ip-precedence-dscp** *dscp1 ... dscp8*

**no mls qos map ip-precedence-dscp**

**default mls qos map ip-precedence-dscp**

| Parameter   | Parameter            | Description                           |
|-------------|----------------------|---------------------------------------|
| Description | <i>dscp1...dscp8</i> | DSCP list. The range is from 0 to 63. |

**Defaults** By default, the IP precedence 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.

**Command** Global configuration mode.

**Mode**

**Usage Guide** N/A

**Configuration** Ruijie(config)# mls qos map ip-precedence-dscp 8 10 16 18 24 26 32 34

**Examples**

| Related  | Command                                         | Description                                 |
|----------|-------------------------------------------------|---------------------------------------------|
| Commands | <b>show mls qos maps</b><br><b>ip-prec-dscp</b> | Displays the IP-precedence to DSCP mapping. |

Platform N/A

Description

## 9.5 mls qos scheduler

Use this command to configure the output queue scheduling. Use the **no** or **default** form of this command to restore the default scheduler.

**mls qos scheduler** [ **sp** | **wrr** ]

**no mls qos scheduler**

|                                        | Parameter  | Description                                                |
|----------------------------------------|------------|------------------------------------------------------------|
| <b>Parameter</b><br><b>Description</b> | <b>sp</b>  | Specifies the absolute priority scheduling.                |
|                                        | <b>wrr</b> | Specifies the frame count weighted round-robin scheduling. |

**Defaults** The default queue scheduling is **wrr**.

**Command Mode** Global configuration mode/interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example specifies the sp scheduling.

**Examples**

```
Ruijie(config)# mls qos scheduler sp
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mls qos scheduler drr
```

|                         | Command                       | Description                           |
|-------------------------|-------------------------------|---------------------------------------|
| <b>Related Commands</b> | <b>show mls qos scheduler</b> | Displays the output queue scheduling. |

**Platform** N/A

**Description**

## 9.6 mls qos trust

Use this command to configure the trust mode on an interface. Use the **no** or **default** form of this command to restore the default setting.

**mls qos trust { cos | dscp | ip-precedence }**

**no mls qos trust**

**default mls qos trust**

|                                        | Parameter            | Description                      |
|----------------------------------------|----------------------|----------------------------------|
| <b>Parameter</b><br><b>Description</b> | <b>cos</b>           | Specifies the CoS trust mode.    |
|                                        | <b>dscp</b>          | Specifies the DSCP trust mode.   |
|                                        | <b>ip-precedence</b> | Specifies the IP-PRE trust mode. |

**Defaults** No trust mode is configured by default.

**Command Mode** Interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example configures the CoS trust mode.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# mls qos trust cos
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     |             |

**Platform**

N/A

**Description**

## 9.7 rate-limit

Use this command to configure rate limiting on the interface. Use the **no** or **default** form of this command to remove rate limiting from the interface.

**rate-limit** { **input** | **output** } *bps* [ *burst-size* ]

**no rate-limit** { **input** | **output** }

**default rate-limit** { **input** | **output** }

**Parameter  
Description**

| Parameter         | Description                                                                           |
|-------------------|---------------------------------------------------------------------------------------|
| <b>input</b>      | Configures input rate limiting.                                                       |
| <b>output</b>     | Configures output rate limiting.                                                      |
| <i>bps</i>        | Bandwidth limit value per second in the unit of KBits, in the range of 16 to 1000000. |
| <i>burst-size</i> | Burst traffic limit value in the unit of KBytes, in the range of 1 to 64.             |

**Defaults**

Rate limiting is not configured by default.

**Command**

Interface configuration mode.

**Mode****Usage Guide**

N/A

**Configuration**

The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 256 Kbps.

**Examples**

```
Ruijie(config)# interface gigabitethernet 0/3
Ruijie(config-if-GigabitEthernet 0/3)# rate-limit input 10240 64
```

**Related  
Commands**

| Command                                                                 | Description                                                |
|-------------------------------------------------------------------------|------------------------------------------------------------|
| <b>show mls qos rate-limit</b> [ <b>interface</b> <i>interface-id</i> ] | Displays the rate limiting configuration of the interface. |

**Platform**

N/A

**Description**



## 9.8 show mls qos maps

Use this command to display DSCP-CoS mapping, CoS-DSCP mapping and IP-PRE-DSCP mapping.

**show mls qos maps [ cos-dscp | dscp-cos | ip-prec-dscp ]**

| Parameter   | Parameter           | Description                       |
|-------------|---------------------|-----------------------------------|
| Description | <b>cos-dscp</b>     | Displays the CoS-DSCP mapping.    |
|             | <b>dscp-cos</b>     | Displays the DSCP-CoS mapping.    |
|             | <b>ip-prec-dscp</b> | Displays the IP-PRE-DSCP mapping. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example displays the CoS-DSCP mapping.

```
Ruijie# show mls qos maps cos-dscp
cos dscp
--- ----
0 0
1 8
2 16
3 24
4 32
5 40
6 48
7 56
```

The fields in the output of this command are described in the following table.

| Field | Description                      |
|-------|----------------------------------|
| cos   | Indicates the CoS value.         |
| dscp  | Indicates the DSCP value mapped. |

The following example displays the DSCP- CoS mapping.

```
Ruijie# show mls qos maps dscp-cos
dscp cos dscp cos dscp cos dscp cos


```

|    |   |    |   |    |   |    |   |
|----|---|----|---|----|---|----|---|
| 0  | 0 | 1  | 0 | 2  | 0 | 3  | 0 |
| 4  | 0 | 5  | 0 | 6  | 0 | 7  | 0 |
| 8  | 1 | 9  | 1 | 10 | 1 | 11 | 1 |
| 12 | 1 | 13 | 1 | 14 | 1 | 15 | 1 |
| 16 | 2 | 17 | 2 | 18 | 2 | 19 | 2 |
| 20 | 2 | 21 | 2 | 22 | 2 | 23 | 2 |
| 24 | 3 | 25 | 3 | 26 | 3 | 27 | 3 |
| 28 | 3 | 29 | 3 | 30 | 3 | 31 | 3 |
| 32 | 4 | 33 | 4 | 34 | 4 | 35 | 4 |
| 36 | 4 | 37 | 4 | 38 | 4 | 39 | 4 |
| 40 | 5 | 41 | 5 | 42 | 5 | 43 | 5 |
| 44 | 5 | 45 | 5 | 46 | 5 | 47 | 5 |
| 48 | 6 | 49 | 6 | 50 | 6 | 51 | 6 |
| 52 | 6 | 53 | 6 | 54 | 6 | 55 | 6 |
| 56 | 7 | 57 | 7 | 58 | 7 | 59 | 7 |
| 60 | 7 | 61 | 7 | 62 | 7 | 63 | 7 |

The fields in the output of this command are described in the following table.

| Field | Description                     |
|-------|---------------------------------|
| dscp  | Indicates the DSCP value.       |
| cos   | Indicates the CoS value mapped. |

The following example displays the IP-PRE-DSCP mapping.

```
Ruijie# show mls qos maps ip-prec-dscp
ip-precedence dscp

0 0
1 8
2 16
3 24
4 32
5 40
6 48
7 56
```

The fields in the output of this command are described in the following table.

| Field         | Description                      |
|---------------|----------------------------------|
| ip-precedence | Indicates the IP-PRE value.      |
| dscp          | Indicates the DSCP value mapped. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

Platform N/A

**Description**

## 9.9 show mls qos queueing

Use this command to display the QoS queuing configuration.

**show mls qos queueing** [ **interface** *interface-id* ]

| Parameter   | Parameter                            | Description      |
|-------------|--------------------------------------|------------------|
| Description | <b>interface</b> <i>interface-id</i> | ID of interface. |

**Defaults** N/A

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the QoS queuing configuration.

**Examples**

```
Ruijie# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0 1
1 2
2 3
3 4
4 5
5 6
6 7
7 8

wrr bandwidth weights:
qid weights
--- -----
1 1
2 2
3 3
4 4
5 5
6 6
7 7
8 8

Interface: GigabitEthernet 0/1
```

```
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
```

The fields in the output of this command are described in the following table.

| Field                 | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| Cos-queue map         | Indicates the mapping between the CoS value and the queue ID. |
| wrr bandwidth weights | Indicates the WRR queue weight.                               |
| cos                   | Indicates the CoS value.                                      |
| qid                   | Indicates the queue ID.                                       |
| weights               | Indicates the weight value                                    |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 9.10 show mls qos rate-limit

Use this command to display the rate limiting configuration of the interface.

**show mls qos rate-limit** [ **interface** *interface-id* ]

| Parameter Description | Parameter           | Description    |
|-----------------------|---------------------|----------------|
|                       | <i>interface-id</i> | Interface name |

**Defaults** N/A

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the rate limiting configuration of all interfaces.

**Examples**

```
Ruijie# show mls qos rate-limit
Interface: GigabitEthernet 0/1
 rate limit input Kbps = 10240 burst = 256
Interface: GigabitEthernet 0/3
 rate limit output Kbps = 102400 burst = 4096
```

The fields in the output of this command are described in the following table.

| Field                               | Description                                         |
|-------------------------------------|-----------------------------------------------------|
| Interface                           | Indicates the interface name.                       |
| rate limit input Kbps = x burst = y | Indicates the input rate limit value, and the input |

|                                      |                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------|
|                                      | burst traffic limit value.                                                       |
| rate limit output Kbps = x burst = y | Indicates the output rate limit value, and the output burst traffic limit value. |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 9.11 show mls qos scheduler

Use this command to display the queue scheduling policy.

**show mls qos scheduler** [ **interface** *interface-id* ]

| Parameter          | Parameter                            | Description          |
|--------------------|--------------------------------------|----------------------|
| <b>Description</b> | <b>interface</b> <i>interface-id</i> | ID of the interface. |

**Defaults** None

**Command Mode** Privileged EXEC mode, global configuration mode, interface configuration mode.

**Usage Guide** N/A

**Configuration** The following example displays the queue scheduling policy.

### Examples

```
Ruijie# show mls qos scheduler
Global Multi-Layer Switching scheduling
Weighted Round Robin
```

The fields in the output of this command are described in the following table.

| Field                | Description                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------|
| Weighted Round Robin | Indicates that the queue scheduling policy is WRR.<br>Other queue scheduling policy:<br>SP: Strict Priority |

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 9.12 wrr-queue bandwidth

Use this command to set the WRR weight ratio. Use the **no** or **default** form of this command to restore the default setting.

**wrr-queue bandwidth** *weight1 ... weight8*

**no wrr-queue bandwidth**

**default wrr-queue bandwidth**

| Parameter   | Parameter                | Description                                                                                                                                                                                                                                             |
|-------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <i>weight1...weight8</i> | 8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15. |

**Defaults** The default queue weight ratio is 1:1:1:1:1:1:1:1.

**Command** Global configuration mode/interface configuration mode.

**Mode**

**Usage Guide** If the weight value is 0, the SP scheduling policy is applied.

**Configuration** The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8.

**Examples**

```
Ruijie(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8
```

```
Ruijie(config)# interface gigabitEthernet 0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)# wrr-queue bandwidth 1 1 2 2 2 2 4 4
```

| Related  | Command                     | Description                             |
|----------|-----------------------------|-----------------------------------------|
| Commands | <b>show mls qos queuing</b> | Displays the QoS queuing configuration. |

**Platform** N/A

**Description**

# Reliability Configuration Commands

---

## 1. RLDP Commands

# 1 RLDP Commands

## 1.1 rldp detect-interval

Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the **no** form or **default** form of this command to restore the default value.

**rldp detect-interval** *interval*

**no rldp detect-interval**

**default rldp detect-interval**

| Parameter Description | Parameter       | Description                                          |
|-----------------------|-----------------|------------------------------------------------------|
|                       | <i>interval</i> | Detection interval in the range from 2 to 15 seconds |

**Defaults** 3 seconds.

**Command Mode** Global configuration mode.

**Usage Guide** In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.

**Configuration Examples** The following example shows how to set the detection interval as 5s:

```
Ruijie(config)# rldp detect-interval 5
```

| Related Commands | Command                | Description                            |
|------------------|------------------------|----------------------------------------|
|                  | <b>rldp detect-max</b> | Sets the maximum number of detections. |

**Platform Description** N/A.

## 1.2 rldp detect-max

Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the **no** form or **default** form of this command to restore it to the default value.

**rldp detect-max** *num*

**no rldp detect-max**

**default rldp detect-max**



|                               |                                                                                                        |                                                        |
|-------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                                                       | <b>Description</b>                                     |
|                               | <i>num</i>                                                                                             | Maximum number of detections in the range from 2 to 10 |
| <b>Defaults</b>               | 2.                                                                                                     |                                                        |
| <b>Command Mode</b>           | Global configuration mode.                                                                             |                                                        |
| <b>Usage Guide</b>            | This command is used together with the detection interval to specify the maximum number of detections. |                                                        |
| <b>Configuration Examples</b> | The following example shows how to set the maximum number of detections as 5:                          |                                                        |
|                               | <pre>Ruijie(config)# rldp detect-max 5</pre>                                                           |                                                        |
| <b>Related Commands</b>       | <b>Command</b>                                                                                         | <b>Description</b>                                     |
|                               | <b>rldp detect-interval</b>                                                                            | Sets the detection interval.                           |
| <b>Platform Description</b>   | N/A.                                                                                                   |                                                        |

### 1.3 rldp enable

Use this command to enable RLDP globally. Use the **no** form or **default** form of this command to disable the function.

**rldp enable**

**no rldp enable**

**default rldp enable**

|                               |                                                                            |                    |
|-------------------------------|----------------------------------------------------------------------------|--------------------|
| <b>Parameter Description</b>  | <b>Parameter</b>                                                           | <b>Description</b> |
|                               | N/A.                                                                       | N/A.               |
| <b>Defaults</b>               | Disabled.                                                                  |                    |
| <b>Command Mode</b>           | Global configuration mode.                                                 |                    |
| <b>Usage Guide</b>            | You can enable RLDP on the interface only when the global RLDP is enabled. |                    |
| <b>Configuration Examples</b> | The following example shows how to enable RLDP:                            |                    |
|                               | <pre>Ruijie(config)# rldp enable</pre>                                     |                    |

| Related Commands | Command | Description            |
|------------------|---------|------------------------|
|                  |         | <code>rldp port</code> |

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

## 1.4 rldp neighbor-negotiation

Use this command to enable RLDP neighbor negotiation. Use the **no** form 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.        |

**Defaults** RLDP neighbor negotiation is disabled by default.

**Command Mode** Global configuration mode.

**Usage Guide** With neighbor negotiation enabled, RLDP unidirectional-/bidirectional-link detection starts only after the neighbor negotiation is successful. (Receiving the Prob message from the neighbor indicates the neighbor negotiation is successful.)

**Configuration Examples** The following example shows how to enable RLDP neighbor negotiation:

```
Ruijie#config
Ruijie(config)#rldp neighbor-negotiation
```

| Related Commands | Command | Description            |
|------------------|---------|------------------------|
|                  |         | <code>rldp port</code> |

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

## 1.5 rldp port

Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the **no** form or **default** form of this command to disable the function.

**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-port | block }**

**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> | Sets unidirectional link detection. |
|                       | <b>bidirection-detect</b>  | Sets bidirectional link detection.  |
|                       | <b>loop-detect</b>         | Sets loop detection type.           |
|                       | <b>warning</b>             | Warns the user.                     |
|                       | <b>shutdown-port</b>       | Shut downs the port.                |

**Defaults** N/A

**Command Mode** Interface configuration mode.

**Usage Guide** The RLDP detection on the port takes effect only when the global RLDP is enabled.

**Configuration Examples** The following example shows how to configure RLDP detection on GigabitEthernet 0/1, specify the detection type as loop detection, and troubleshooting method as block.

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# rldp port loop-detect block
```

| Related Commands | Command            | Description            |
|------------------|--------------------|------------------------|
|                  | <b>rldp enable</b> | Enables RLDP globally. |

**Platform Description** N/A.

## 1.6 rldp reset

Use this command to make all the ports that have been handled using rldp shutdown or disable to perform RLDP detection again.

**rldp reset**

| <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 example below demonstrates how to use this command:

```
Ruijie# rldp reset
```

| <b>Related Commands</b> | Command     | Description            |
|-------------------------|-------------|------------------------|
|                         | rldp enable | Enables RLDP globally. |

**Platform Description** N/A.

## 1.7 show rldp

Use this command to display the RLDP information.

**show rldp [ interface *interface-id* ]**

| <b>Parameter Description</b> | Parameter           | Description  |
|------------------------------|---------------------|--------------|
|                              | <i>interface-id</i> | Interface ID |

**Defaults** N/A.

**Command Mode** Privileged EXEC mode.

**Usage Guide** N/A.

**Configuration Examples** The following example displays the RLDP information.

```
Ruijie# show rldp interface GigabitEthernet 0/40
port state : normal
local bridge : 00d0.f822.3362
neighbor bridge : 0000.0000.0000
neighbor port :
```

```
loop detect information:
 action: shutdown-port
 state : normal
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A.    | N/A.        |

**Platform  
Description**

N/A.

## Network Monitoring Configuration Commands

---

1. SNMP Commands
2. NTP Commands
3. SPAN-RSPAN Commands

# 1 SNMP Commands

## 1.1 no snmp-server

Use this command to disable the SNMP agent function.

**no snmp-server**

| Parameter<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          | N/A       | N/A         |

**Defaults** SNMP agent is enabled by default.

**Command mode** Global configuration mode.

**Usage Guide** This command disables the SNMP agent services of all versions supported on the device.

**Configuration Examples** The following example disables the SNMP agent.

```
Ruijie(config)# no snmp-server
```

| Related<br>Commands | Command | Description |
|---------------------|---------|-------------|
|                     | N/A     | N/A         |

**Platform Description** N/A

## 1.2 show snmp

Use this command to display the SNMP configuration.

**show snmp [ mib | user | view | group | host | process-mib-time ]**

| Parameter<br>Description | 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>process-mib-time</b> | Displays the MIB node requiring the longest processing time. |

**Defaults** N/A

**Command mode** Privileged EXEC mode.

**Usage Guide** N/A

**Configuration** The example below displays the SNMP configuration:

**Examples**

```
Ruijie# 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
```

**Related Commands**

| Command                       | Description                                |
|-------------------------------|--------------------------------------------|
| <b>snmp-server chassis-id</b> | Specifies the SNMP system sequence number. |

**Platform** N/A

**Description**

### 1.3 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<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          |           | 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.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no snmp trap link-status
```

The following example enables the interface to send link traps.

```
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# snmp trap link-status
```

| Related<br>Commands | Command | Description |
|---------------------|---------|-------------|
|                     |         | N/A         |

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

## 1.4 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<br>Description | Parameter | Description |
|--------------------------|-----------|-------------|
|                          |           | <i>text</i> |

**Defaults** The default is 60FF60.

**Command** Global configuration mode.  
**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** The following example specifies the SNMP chassis ID as 123456:

**Examples** Ruijie(config)# **snmp-server chassis-id 123456**

**Related  
Commands**

| Command          | Description                      |
|------------------|----------------------------------|
| <b>show snmp</b> | Displays the SNMP configuration. |

**Platform** N/A

**Description**

## 1.5 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* [ **view** *view-name* ] [ [ **ro** | **rw** ] [ **host** *ipaddr* ] ] [ *aclnum* | *aclname* ]

**no snmp-server community** [ 0 | 7 ] *string*

**Parameter  
Description**

| Parameter        | Description                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>0</b>         | Indicates that the community string is in plaintext.                                                                      |
| <b>7</b>         | 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.                                 |
| <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>    | Access list number (1 to 199, and 1300 to 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>ipaddr</i>    | Specifies the IP address of the NMS to access the MIB.                                                                    |

**Defaults** All communities are read only by default.

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

```
Ruijie(config)# snmp-server community public ro
```

| Related Commands | Command | Description        |
|------------------|---------|--------------------|
|                  |         | <b>access-list</b> |

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

## 1.6 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 Examples** The following example specifies the SNMP system contract i-net800@i-net.com.cn:

```
Ruijie(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**

## 1.7 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.

```
Ruijie(config)# password policy min-size 6
Ruijie(config)# snmp-server enable secret-dictionary-check
Ruijie(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 Description** N/A

## 1.8 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 [ notification-type ]**

| Parameter Description | Parameter                | Description                                                               |
|-----------------------|--------------------------|---------------------------------------------------------------------------|
|                       | <i>notification-type</i> | Specifies the type of trap messages.<br>entity: SNMP entity trap message. |

|  |                                                                                                 |
|--|-------------------------------------------------------------------------------------------------|
|  | snmp: SNMP trap message.<br>bridge: Bridge trap message.<br>mac-notification: MAC 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**

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(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**

## 1.9 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**

```
Ruijie(config)# snmp-server flow-control pps 200
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform** N/A

**Description**

## 1.10 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* ]

**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. |

**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**

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                        |                                        |
|------------------------|----------------------------------------|
| <b>show snmp group</b> | Displays the SNMP group configuration. |
|------------------------|----------------------------------------|

**Platform** N/A

**Description**

### 1.11 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* } [ **traps** | **informs** ] [ **version** { 1 | 2c | 3 { **auth** | **noauth** | **priv** } } ] *community-string* [ **udp-port** *port-num* ] [ *notification-type* ]

**no snmp-server host** { *host-addr* } [ **traps** | **informs** ] [ **version** { 1 | 2c | 3 { **auth** | **noauth** | **priv** } } ] *community-string* [ **udp-port** *port-num* ]

**Parameter Description**

| Parameter                                 | Description                                                                                                                                                        |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host-addr</i>                          | SNMP host address.                                                                                                                                                 |
| <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.                                                                                                                                             |
| <i>notification-type</i>                  | The type of the SNMP trap message, such as <b>snmp</b> .<br>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.  
Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured.

**Configuration Examples** The following example specifies an SNMP host to receive the SNMP event trap:

```
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

**Related Commands**

| Command | Description |
|---------|-------------|
|---------|-------------|

|                                 |                                                       |
|---------------------------------|-------------------------------------------------------|
| <b>snmp-server enable traps</b> | Enables the SNMP agent to send the SNMP trap message. |
|---------------------------------|-------------------------------------------------------|

**Platform** N/A

**Description**

## 1.12 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**

| Parameter Description | Parameter        | Description                                                            |
|-----------------------|------------------|------------------------------------------------------------------------|
|                       | <i>retry-num</i> | Specifies the resend times for inform requests, ranging from 0 to 255. |
|                       | <i>time</i>      | Specifies the inform request timeout, 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 Examples** The following example configures the resend times of inform requests to 5.

```
Ruijie(config)# snmp-server inform retries 5
```

The following example configures the inform request timeout to 20 seconds.

```
Ruijie(config)# snmp-server inform timeout 20
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 1.13 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**

```
Ruijie(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** N/A

**Description**

## 1.14 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:

```
Ruijie(config)# snmp-server packetsize 1492
```

**Configuration** N/A

**Examples****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**

## 1.15 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** The following example specifies the length of message queue as 100.**Examples**

```
Ruijie(config)# snmp-server queue-length 100
```

**Related  
Commands**

| Command                       | Description                                    |
|-------------------------------|------------------------------------------------|
| <b>snmp-server packetsize</b> | Specifies the largest size of the SNMP packet. |

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

## 1.16 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**

The following example enables the SNMP message reload function:

**Examples**

```
Ruijie(config)# snmp-server system-shutdown
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 1.17 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* | **ip** *ip-address* }

**no snmp-server trap-source** [ **ip** ]

**Parameter  
Description**

| Parameter                   | Description                                               |
|-----------------------------|-----------------------------------------------------------|
| <i>interface</i>            | Specifies the source interface of the SNMP trap message.  |
| <b>ip</b> <i>ip-address</i> | Specifies the source IP address of the SNMP trap message. |

**Defaults**

By default, the IP address of the interface from which the SNMP packet is sent is just the source address.

**Command  
mode**

Global configuration mode.

**Usage Guide**

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:

```
Ruijie(config)# snmp-server trap-source gigabitethernet 0/1
```

**Related Commands**

| 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 Description** N/A

## 1.18 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 *time***

**no snmp-server trap-timeout**

**Parameter Description**

| Parameter   | Description                                                                                                                     |
|-------------|---------------------------------------------------------------------------------------------------------------------------------|
| <i>time</i> | The retransmission timeout is set to be the <i>time</i> value multiplied by 10ms. The <i>time</i> value ranges from 1 to 1,000. |

**Defaults** The default *time* value is 30, namely, the default retransmission timeout is 300ms,

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example specifies the timeout period as 600ms.

```
Ruijie(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**

## 1.19 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 range is from 1 to 65,535. |

**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**

```
Ruijie(config)# snmp-server udp-port 15000
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

Description

## 1.20 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] }
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   v2c   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. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 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.                                                                                                                                                                                                                                                                                                                 |
| <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. <i>des56</i> 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.                                                                                                                            |
| <b>md5</b>           | Enables the MD5 authentication protocol. While the <b>sha</b> enables the SHA authentication protocol.                                                                                                                                                                                                                                                               |

**Defaults** N/A

**Command mode** Global configuration mode.

**Usage Guide** N/A

**Configuration Examples** The following example configures an SNMPv3 user with MD5 authentication and DES encryption:

```
Ruijie(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv
```

```
des56 despassstr
```

**Related  
Commands**

| Command               | Description                           |
|-----------------------|---------------------------------------|
| <b>show snmp user</b> | Displays the SNMP user configuration. |

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

## 1.21 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** The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).**Examples**

```
Ruijie(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** N/A**Description**

## 2 NTP Commands

### 2.1 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 authentication is configured, the NTP service will be enabled.

**Configuration Examples** The following example disables NTP.

```
Ruijie(config)#no ntp
```

| Related Commands | Command    | Description              |
|------------------|------------|--------------------------|
|                  | ntp server | Specifies an NTP server. |

**Platform Description** N/A

### 2.2 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.

```
Ruijie(config)#ntp authentication-key 6 md5 woooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(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 Description** N/A

## 2.3 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 4,294,967,295.                                                                                                                             |
| <i>key-string</i> | Key string.                                                                                                                                                          |
| <i>enc-type</i>   | (Optional) 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**

```
Ruijie(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**

## 2.4 ntp disable

Use this command to disable the device to receive NTP packets on the specified interface.

**ntp disable**

**Parameter Description**

| Parameter | Description |
|-----------|-------------|
| N/A       | N/A         |

**Defaults** All NTP packets can be received by default.

**Command mode** Interface configuration mode.

**Usage Guide** The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface.

By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.

 This command is configured only the interface that can receive and send IP packets.

**Configuration** The following example disables the device to receive the NTP packets.

**Examples**

```
Ruijie(config-if-VLAN 1)# no ntp disable
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

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

## 2.5 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 } [version version] [source if-name] [key keyid]
[prefer]
no ntp server ip-addr
```

| Parameter Description | Parameter      | Description                                                                                                                                    |
|-----------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <i>ip-addr</i> | Sets the IP address of the NTP server. The address can be in IPv4 format.                                                                      |
|                       | <i>domain</i>  | Sets the domain name of the NTP server, supporting IPv4.                                                                                       |
|                       | <i>version</i> | (Optional) Specifies the NTP version (1-3). The default is NTPv3.                                                                              |
|                       | <i>if-name</i> | (Optional) Specifies the source interface from which the NTP message is sent (L3 interface).                                                   |
|                       | <i>keyid</i>   | (Optional) 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>  | (Optional) Specifies the given NTP server as the preferred one.                                                                                |


**Defaults** No NTP server is configured by default.

**Command mode** Global configuration mode.

**Usage Guide** At present, RGOS system 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: `Ruijie(config)# ntp server 192.168.210.222`

| Related Commands | Command             | Description |
|------------------|---------------------|-------------|
|                  | <code>no ntp</code> |             |

**Platform** N/A

**Description**

## 2.6 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> |             |

**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**

```
Ruijie(config)#ntp authentication-key 6 md5 woooooop
Ruijie(config)#ntp trusted-key 6
Ruijie(config)#ntp server 192.168.210.222 key 6
```

| Related Commands                    | Command                       | Description                           |
|-------------------------------------|-------------------------------|---------------------------------------|
|                                     | <code>ntp authenticate</code> |                                       |
| <code>ntp authentication-key</code> |                               | Configures an NTP authentication key. |
| <code>ntp server</code>             |                               | Configures an NTP server.             |

**Platform** N/A

**Description**

## 2.7 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**

**Parameter Description**

| 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**

```
Ruijie(config)# ntp update-calendar
```

**Related Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform**

N/A

**Description**

## 2.8 show ntp server

Use this command to display the NTP server configuration.

**show ntp server**

**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** N/A

**Configuration** The following example displays the NTP server.

**Examples**

```
Ruijie# show ntp server
ntp-server source keyid prefer version

192.168.210.222 None None FALSE 3
```

| Related Commands | Command | Description |
|------------------|---------|-------------|
|                  | N/A     | N/A         |

**Platform** N/A

**Description**

## 2.9 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**

```
Ruijie# 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

## 3 SPAN-RSPAN Commands

### 3.1 monitor session

Use this command to configure the SPAN session and specify the source port (monitored port).

**monitor session** *session-num* **source interface** *source-interface-id* [ **both** | **rx** | **tx** ]

Use this command to configure the SPAN session and specify the destination port (monitoring port).

**monitor session** *session-num* **destination interface** *destination-interface-id* [ **switch** ]

Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.

**no monitor session** { **all** | *session-num* [ **source interface** *source-interface-id* [ **both** | **rx** | **tx** ] / **destination interface** *destination-interface-id* [ **switch** ] ] }

Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.

**default monitor session** { **all** | *session-num* { **source interface** *source-interface-id* [ **both** | **rx** | **tx** ] / **destination interface** *destination-interface-id* [ **switch** ] } }

#### Parameter Description

| Parameter                       | Description                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------|
| <i>session_number</i>           | Indicates the SPAN session number, ranging from 1 to 4.                               |
| <i>source-interface-id</i>      | Specifies the source interface, which can be one interface or a range of interfaces.  |
| <i>destination-interface-id</i> | Specifies the destination interface.                                                  |
| <b>rx</b>                       | Monitors the only received traffic.                                                   |
| <b>tx</b>                       | Monitors the only transmitted traffic.                                                |
| <b>both</b>                     | Monitors both received and transmitted traffic. This is the default.                  |
| <b>switch</b>                   | Enables switching on the destination port. Switching function is disabled by default. |
| <b>all</b>                      | Indicates all monitor sessions.                                                       |

**Defaults** Port monitoring is disabled by default.

**Command mode** Global configuration mode.

**Usage Guide** Use this command to configure SPAN or remote SPAN, and specify the source port or destination port.



If the **both**, **rx** or **tx** is not specified for the source port, the **both** parameter is the default.  
The **switch** feature is disabled on the destination port.

**Configuration** The following example configures the source port and destination port of the SPAN session.

**Examples**

```
Ruijie(config)# monitor session 1 source interface gigabitethernet 0/1
Ruijie(config)# monitor session 1 destination interface gigabitethernet 0/2
```

The following example removes the SPAN session.

```
Ruijie(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
Ruijie(config)# no monitor session 1 source interface gigabitethernet 0/1
Ruijie(config)# no monitor session 1 destination interface gigabitethernet
0/2
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

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

## 3.2 show monitor

Use this command to display the SPAN configurations.

**show monitor** [ **session** *session\_number* ]

**Parameter  
Description**

| Parameter             | Description                                               |
|-----------------------|-----------------------------------------------------------|
| <i>session_number</i> | Displays the specified SPAN session, ranging from 1 to 4. |

**Defaults** N/A

**Command mode** Privileged EXEC mode, global configuration mode and interface configuration mode

**Usage Guide** N/A

**Configuration** This following example displays all SPAN sessions.

**Examples**

```
Ruijie(config)# show monitor
sess-num: 1
span-type: LOCAL_SPAN
```

```
src-intf:
GigabitEthernet 0/1 frame-type Both
dest-intf:
GigabitEthernet 0/2
sess-num: 2
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/3 frame-type Both
dest-intf:
GigabitEthernet 0/4
```

The following example displays SPAN session 1.

```
Ruijie(config)# show monitor session 1
sess-num: 1
span-type: LOCAL_SPAN
src-intf:
GigabitEthernet 0/1 frame-type Both
dest-intf:
GigabitEthernet 0/2
```

**Related  
Commands**

| Command | Description |
|---------|-------------|
| N/A     | N/A         |

**Platform  
Description**

N/A